DOCTOR OF PHILOSOPHY

Examination of identity theft and identity fraud and the role of the national identity card scheme

Holmes, Tim

Award date:
2009

Awarding institution:
Bangor University

Examination of Identity Theft and Identity Fraud and the Role of the National Identity Card Scheme

Timothy Holmes
2009

A thesis submitted in fulfilment of the requirement for the Degree of Doctor of Philosophy

School of Social Sciences
College of Business, Social Science and Law
Bangor University

Acknowledgements

I am very grateful to my supervisor Graham Day, for all the support, direction and advice that he has given me. I would also like to thank everyone at the School of Social Sciences, in particular Howard Davis, Ann McLaren, Preet Nijhar, Julia Wardhaugh and Brenda Clare. Thank you to all my fellow students and friends at the School of Social Sciences for making Bangor a great work environment.

Acknowledgement should also go to the following organisations, namely – The Conservative Party, DEFY-ID, Experian, Equifax, Identity and Passport Service Justice, Not Vengeance, Knights Bridge Castle Group, the Labour Party, Liberal Democrats party, NO2ID, Privacy Rights Clearing House, Privacy International, Liberty and the Red Cross. These are organisations who have helped me both directly and indirectly with this study. Their willingness to speak to me has been greatly appreciated. My search was done in great part using the internet and I am aware that these organisations had no obligation to answer any of my enquiries. I would like to mention the following people for their assistance - Sarah Airey, James Blindell, Chris Broggan, Ian Brown, Charles Clarke MP, Emily Finch, Beth Givens, Matthew Hanney, Rikke Frank Joergensen, Tim Logan, Anni Lennox, Lesley Malone, Megan McNally, Trevor Mendham and Natasha Semmens.

Finally I would like to thank my family, my sister Eleri and mum Angharad for their support and encouragement over the years, but mostly I think my dad Adrian deserves the credit for this study. Five years ago he suggested I study identity fraud and since then he has been an invaluable sounding board for ideas and arguments.

Abstract

Since the start of the 21st century the terms identity theft and identity fraud have been used to describe a variety of crimes which appear both new and unique to the 21st century. So much so, that the government is in the process of re-introducing a National Identity Card Scheme to tackle the problem. But are identity theft and identity fraud uniquely 21st century problems, and is a new Identity Card Scheme going to prevent these crimes?

The study seeks to examine identity theft and identity fraud and determine what these crimes are, and to distinguish between the two. In order to do this, the study will examine the different definitions used in America, Australia and the U.K. as well as the history of identity related crime. The use of identity theft and identity fraud by organised crime, illegal immigration and terrorism will also be discussed. This examination of identity theft and identity fraud includes an explanation of the differences between modern and traditional identity related crimes and the various methods used to gather information on people's identities.

The study also looks at ways of researching identity related crime. As part of the research process, simulated identity theft was developed as a research approach. The use of this research method and the ethical and legal consideration associated with it are discussed at length as is the use of the internet as a source of information.

The study concludes with an analysis of the role of the National Identity Card Scheme in preventing identity related crime, and the potential benefits and drawbacks of reintroducing a National Identity Card Scheme.

TABLE OF CONTENTS

CHAPTER 1

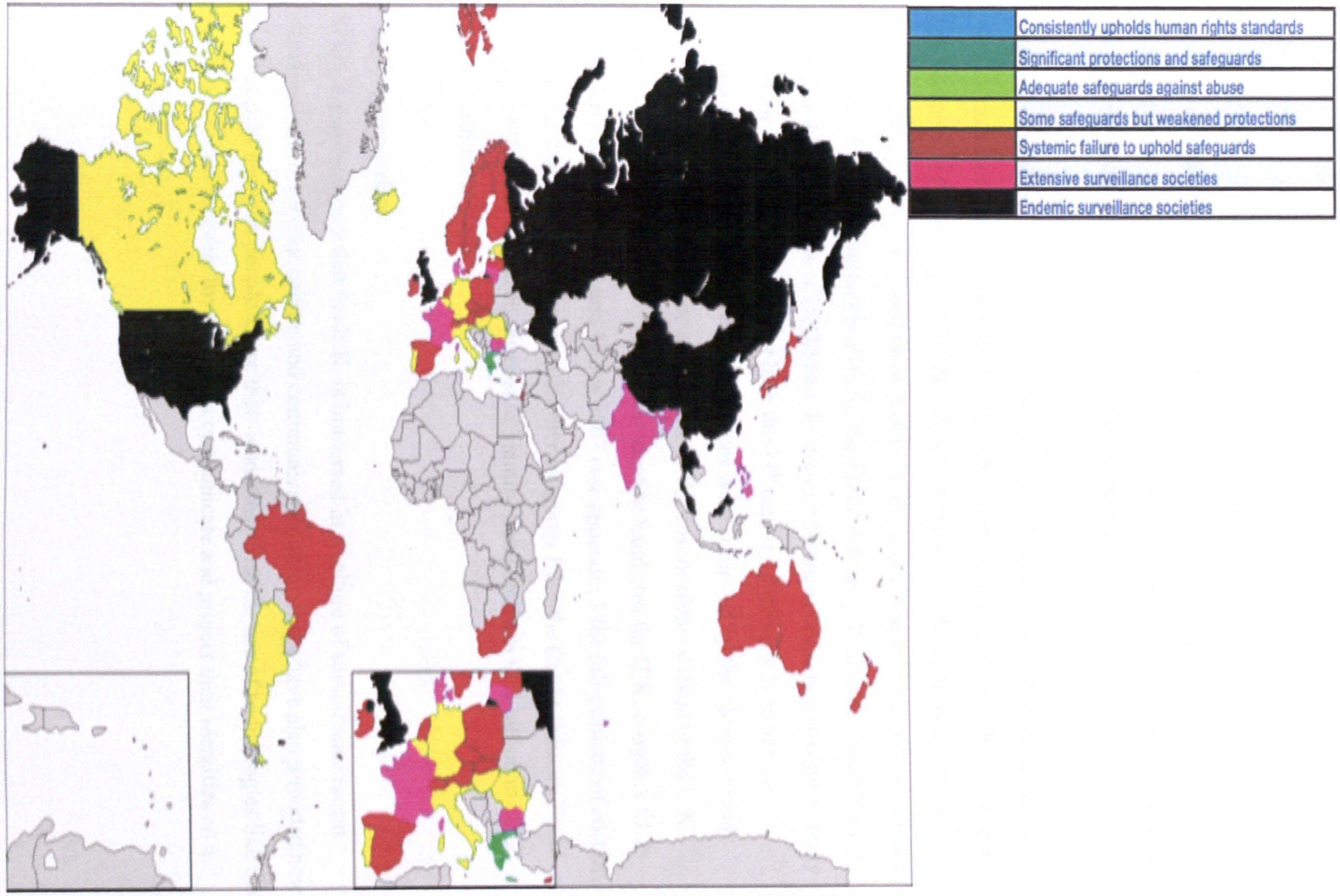
Age of surveillance

In 2004 Barry Steinhardt the director of the Technology and Liberty Program at the American Civil Liberties Union went before the U.S Congress Commerce, Trade and Consumer Protection subcommittee of the House Committee on Energy and Commerce. He presented his organisations views on the use of Radio Frequency Identifiers (R.F.IDs) – small tags which can be used to track people or objects. Steinhardt went before the committee to highlight the risks R.F.ID tags and advances in surveillance technology posed to people's privacy.

> "The explosion of computers, cameras, sensors, wireless communication, GPS, biometrics, and other technologies in just the last 10 years is feeding what can be described as a surveillance monster that is growing silently in our midst. Scarcely a month goes by in which we don't read about some new high-tech method for invading privacy, from face recognition to implantable microchips, data-mining to DNA chips, and now RFID identity tags. The fact is, there are no longer any *technical* barriers to the creation of a surveillance society."
> (Steinhardt .B, 2004: 1)

In the remainder of Steinhardt's statement, he discusses how important it is that in an age where a surveillance society is technically possible, it is important that there are social constraints to protect privacy. Since Steinhardt's statement in 2004, surveillance technology has developed even further. R.F.ID chips can now be implanted in a person's body and biometric security is becoming a common method of confirming identity. While it is debateable whether or not we now live in a surveillance society, it is fair to say we live in an age where the potential to use surveillance is great. The 21st century can be seen as an age of surveillance it is technically possible to track people and monitor them 24/7. In the U.K surveillance technology is a popular tool for crime detection and prevention. A world map produced by Privacy International in 2007 to illustrates how much surveillance people are under around the world in 2006.

Map of Surveillance Societies around the world



Map developed from http://english.freemap.jp

(Privacy International 2007: 1)

In Privacy International's survey it was determined that the U.K. had one fifth of the worlds CCTV cameras and that surveillance was endemic in the U.K. Steinhardt argued in 2004 that society needed social barriers to the protect people from the excessive amounts of state surveillance. But in looking at the way the U.K. has embraced surveillance technology over the past twenty years it can be argued that we as a society are open to the idea of creating a surveillance society.

Curiously, however just as our acceptance of and reliance on surveillance technology in the U.K. has increased, so too have the opportunities to commit identity fraud. Despite the increased use of surveillance technology there is also evidence to suggest that the U.K. is coming under increased threat from identity theft. According to the Association of Payment Clearing Services (APACS), the Fraud Advisory Panel, the Credit Industry Fraud Avoidance System (CIFAS) and the credit reference company Experian, identity fraud is an emerging threat to people in the 21st century. Statistics from various government agencies and private associations were compiled by the Identity Fraud Steering Committee to produce an estimate of the cost of identity fraud to the U.K. economy. The committee determined that identity fraud cost the U.K. economy £1.2 billion between April 2006 and March 2007 (see appendix 1 for full estimate of cost of identity fraud to the U.K. economy). Earlier estimates from the Credit Industry Fraud Avoidance System had placed the cost of identity fraud between £1.3 billion in 2002 and £1.7 billion in 2006.

'Age of perception'

While it can be argued that the U.K. is immersed in a culture of surveillance recent developments in popular culture and communication technology have also provided new and different ways for people to use their identities. With the use of technologies like the internet it is now possible for people to communicate and project their identities on a global scale.

Through the internet, it is now possible for people to form new, virtual identities or to present their identities on a global scale. On the internet there is freedom for individuals to be anyone they want to be, to communicate with anyone who has access to the internet, and enter identification processes without face-to-face interactions. It can be argued that through this technology, society has developed to create an 'age of perception', where people are whoever they want to be.

Social networking websites such as MySpace, Facebook and Bebo have become popular venues for people to express themselves self to any others on the internet. In the online world of Second Life, people can build new virtual identities and homes.

Not only does the internet allow for the use of a person's identity on a global scale it also allows for commercial transactions resulting in private and public organisations forming websites which allow access without face-to-face transactions. While face-to-face interactions are still used in many identification processes, the developments in communication technology have allowed for an alternative. However, the disadvantages of the freedom for people to be whoever they want to be, on the internet, is the rise in identity fraud witnessed in America, Australia and the U.K. in the 21st century. While deception and impersonation have been used by criminals for centuries, it is in the 21st century that the crime of identity fraud has come to prominence.

In the 21st century the U.K. has become in many respects a contradictory nation. On the one hand, the U.K. is a surveillance society; but it is also a society which allows for a great deal of freedom with regard to people's identities. This contradiction is, however reaching a tipping point; the use of surveillance technology to prevent impersonation is now being planned in the form of a National Identity Card Scheme. With the identity card, the U.K. government plans to prevent identity fraud, in effect limiting the degree to which people can use their identities or the identities of other people.

Aims of this study

This study seeks to research what will happen when the U.K.'s use of surveillance technology begins to affect people's ability to deceive with regard to their identities. The initial aim of this study was in many respects a simple one – to explore whether identity cards will stop identity fraud. However, this question raised, within it several even bigger questions: What is identity fraud? What effect can identity cards have on society? Will identity cards prevent crime? What will the identity card actually do? Thus in the attempt to answer one simple question, several more complex questions must be answered first.

Additionally, there are numerous questions surrounding the National Identity Card Scheme. This is the first time that a National Identity Card system has been proposed as a means of stopping crime. It is the first time that biometric security and a biometric database have been suggested on a national scale and this represents a significant step forward in creating a surveillance society. Furthermore given that identity fraud is such a complex, and in some respects 'new' crime, it is difficult to see how there can be anything but questions over what the identity card will and will not do.

Much of the discussion about and opposition to the identity card scheme has been rooted in its implications with respect to civil liberty. Concerns over the creation of a surveillance society as described in George Orwell's book *'1984'* have, it can be argued, distracted people from the real question of whether or not an identity card scheme will actually work. This focus on the implications of the identity cards for civil liberty, rather than on their practical use, can be explained to a certain degree by identifying the origins of the most recent call for identity cards.

Identity cards are arguably a reaction to concern over crimes such as terrorism, illegal immigration, and identity fraud. The beginning of the 21st century has been marked by several dramatic incidents involving these areas of criminal activity. On 11th of September 2001, terrorist attacks using commercial jets on the World Trade Centre and the Pentagon sparked an increased concern with regard to terrorism. In 2004, 21 illegal

immigrants were killed while picking cockles in Morecambe Bay, U.K, bringing to the public's attention the issue of illegal immigrants and the conditions they live and work in. Coupled to these events was the false arrest of Derek Bond in 2003 for the crimes of his impersonator Derek Lloyd Sykes.

These events and others like them have created a 'perfect storm' of fear and concern over defrauding and lying during identification processes and the dangers posed by those who abuse it. This fear of what people who conceal their identity can do has motivated the government to enact several new approaches to terrorism, illegal immigration and the use of fraud. Legislation to protect against terrorist attacks has been enacted the 2001 Anti Terrorism, Crime and Security Act 2001, the Prevention of Terrorism Act of 2005, and the 2006 Terrorism Act. Also, concern for border security has lead to the creation of the U.K. Border Agency, and in 2007 Prime Minister Gordon Brown outlined plans to create a border police force. The new Fraud Act 2006 has been brought into improve law enforcement efforts to combat the innovations in committing fraud that have emerged in the 21st century, such as the use of internet.

The one phenomenon which will be central to this study is the proposed introduction of a National Identity Card Scheme. While it can be argued that other approaches to dealing with terrorism, illegal immigration and identity fraud have been tested, the use of a National Identity Card Scheme as a method of preventing crime is an untested approach. The question must be asked – will it work? As with anything which seeks to predict the future, this study cannot provide concrete answers to the question. It is hoped, however, that by discussing the relevant issues and hypothesising about how identity cards will affect identity fraud significant insight can be gained into the changes that may occur in society with the introduction of the National Identity Card Scheme.

While it may appear that identity fraud is a new phenomenon for the 21st century, history records many impostors and identity thieves. Royal families have had to deal with usurpers, people who have claimed to be missing royals or the true regents. Similarly, looking at famous incidents of fraud and deception, it is possible to see

examples of people who have committed crimes which can be described as identity fraud, before the term not existed. For example, the activities of Frank Abagnale, F.W.Demara and Arthur Orton (see chapter 6) can all be seen as incidents of both identity theft and identity fraud despite their activities not being described as such.

By looking back through history, therefore, it is possible to find several accounts of people who stole the identity of others or who used deception to hide their own identities. Lying about who you are is not a new phenomenon; identity fraud is not a new crime. Nevertheless, it was not until the beginning of the 21st century that people in the U.K. began to perceive identity fraud as a crime. The emergence of the terms identity fraud and identity theft can in part be traced to difficulties faced with this type of crime in America during the 1990s.

This study is split into two parts. In the first part of this study literature on the importance of identification and trust, definitions of identity fraud and background of the National Identity Card Scheme will be discussed. The second part of this study focuses on the methods used in this study, explaining the difference between identity theft and identity fraud and the potential impact of a National Identity Card Scheme on the crimes of identity theft and identity fraud. Due to their importance to the study of identity related crime three high profile cases of identity theft are also included. These sections document the experiences of Michelle Brown and Derek Bond as victims of identity theft and the activities of Charles Stopford and his impersonation of Christopher Buckingham. These cases are of particular importance as they have been influential in raising the profile of identity theft and mention is made of them throughout the study.

Part 1

- Chapter 1 Introduction
- Chapter 2 Importance of Identification and Trust
- Chapter 3 Definitions of Identity Fraud
- Chapter 4 Background of the National Identity Card Scheme

Part 2

- Michelle Brown Case
- Derek Bond Case
- Christopher Buckingham Case
- Chapter 5 Research Methodology
- Chapter 6 History of Identity Theft and Identity Fraud
- Chapter 7 Identity Fraud Progression 1: Gathering and Appropriating
- Chapter 8 Identity Fraud Progression 2: Modern Identity Theft and Modern Identity Fraud
- Chapter 9 Identity Cards vs. Identity Crime
- Chapter 10 Conclusion

Chapter 2

The Importance of Identification and Trust

Central to the argument for the introduction of a National Identity Card Scheme is the idea that the identification processes used in the U.K. today are under threat from criminal activity. Whether this threat should be worried about to the point of introducing new laws and an identity card scheme will be discussed in chapters 3 and 4. However, before discussing the threat posed by identity related crime it is important to look at the identification process and the importance of identification.

In this thesis it is argued that in the 21st century there has been an increase in concern over identification in the U.K. How people identify themselves, and the accuracy of that identification has come under increased scrutiny due to high profile identity related crimes by terrorists, illegal immigrants and professional criminals. The terrorist attacks by Islamic extremists on New York in 2001, and subsequent attacks, have raised concern over accurately identifying people who are a threat to society. Concern over illegal immigration has increased attention given to the question of who is a legitimate citizen and issues of access to government services, and the activities of organised and professional identity thieves have raised concern over the formation of bonds of trust and transactions between individuals. Arguably, the government is seeking to use the National Identity Card Scheme to reinforce and secure the processes of identification used in the U.K, to counter these types of attack. Equally the backlash against the identity card scheme is a further example of anxiety with regard to control of the identification process.

Even without the recent rise in concern with regard to identity and identification the concept of identity and the process of identification is still an important phenomenon. Jenkins (2004) argues that identity and identification are vital:

> "Levels of concern about identity may wax and wane, but, whether individually or collectively, we can't live routine lives as humans without identification, without knowing – and sometimes puzzling about – who we are and who others are. This is true no matter where we are, or what the local way of life or language. Without repertoires of identification we would not be able to relate to each other meaningfully or consistently. We would not have the vital sense of who's who and what's what. Without identity there could be no human world."
> (Jenkins .R, 2004: 7)

When discussing identification and the process by which people identify themselves, social identity, social trust and the use of social symbolism are important factors to consider. The influence of globalisation in the form of new technology such as the World Wide Web is also important to discuss. The use of non-face-to-face interactions such as those experienced via the internet makes it easier to commit identity related crime, as establishing an identity is easier and confirming the validity of the identity is harder.

Social identity theory

One theoretical view of identity and the formation of identity which is important to the study of identity related crime and the identity card scheme is social identity theory. Social identity theory was developed by social psychologists Tajfel and Turner (1979) in their study of the psychological basis of inter-group discrimination (Turner, 1999: 6). According to social identity theory, individuals do not have a single identity; rather they have several identities that correspond to widening circles of group membership. Fulcher and Scott (1999) distinguish between a social identity and self. They argue that individuals are placed into categories of people, and these form social identities (e.g. child, mother, Christian, plumber, thief, homosexual, etc.). Connected to the concept of self is the existence of a personal identity which is used to identify an individual from a particular social group. A clear example of this is a person's name, which indicates that while people may be members of a social group, they are also unique individuals with traits that cannot be covered by social identity:

> "A social identity marks people out as, in certain respects, the same as others. A personal identity marks someone out as a unique and quite distinct individual." (Fulcher .J, Scott .J, 1999: 125)

Discussion of social identity is important in understanding the identification process as it emphasises the role of individuals in choosing how society sees them. Social psychologists highlight the role of the individual in the determining how their identity is formed. Social identity refers to the practice of joining and claiming membership of certain social groups by individuals, and it is important to discuss social identity when looking at identity related crime. In modern cases of identity related crime, the activities of criminals are usually focused on exploiting an individual's membership of a social group. The goal is not to adopt a victim's sense of self or take their personal identity; rather, it is to use their identity to give the false impression that the identity thief is a member of a particular social group.

Consider the case of Derek Lloyd Sykes and his use of Derek Bond's identity (see page 113 for details). Sykes obtained a passport in Bond's name and from this one aspect of Bond's identity, Sykes was able to engage in a lucrative criminal enterprise. Sykes did not need to steal Bond's personal identity, as his goal was simply to give the impression that he was a trustworthy businessman. So limited was the contact that Sykes had with Bond's personal identity, Bond was kept unaware of the theft of his identity for over 20 years. Sykes had used Bond's social identity to protect himself from detection whilst committing criminal activity.

This practice of hijacking people's access to social groups can also be seen in other cases of identity theft such as illegal immigrants using stolen passports or internet based thieves sending phishing emails. The goal is not to take over the victim's sense of self; rather it is to appear as a legitimate member of a social group, or to avoid inclusion in a social group. It is the identification which most identity thieves seek and not the personal identity of the victim. A theory associated with social identity theory is self

categorisation theory; this theory is also important to discuss as it further highlights the role of individuals in choosing their own identity.

Self categorisation theory

While an individual cannot have a valid identity without the confirmation of society, it can also be argued that to some extent it is up to individuals to determine what their identity is. It is argued by Turner (1987) that identity is created by individuals deciding which social group they belong to. Self categorisation theory argues that individuals are responsible for forming their identity:

> "Turner and his colleagues' theory claims that identity is shaped by self-categorization; by people looking at social categories, and deciding whether or not they are in a category. If they consider themselves a member of a category, that category becomes part of their identity. The explanation given by Turner's self categorisation theory works like this:
>
> 1. We see people as members of social categories.
> 2. We also see ourselves as members of social categories.
> 3. We take on identities appropriate to the social categories with which we identify." (Gove, Watt, in Woodward .K, 2000: 47)

It can be argued that self categorisation theory is an important aspect of the study of identity related crime as many examples of identity related crime involve people who consider, or pretend to consider, themselves to be members of social groups or categories that they have no legitimate claim to. In chapter 6, the history of identity theft and identity fraud is discussed with reference to several historical examples of identity related crime. In these examples (of identity related crime) there are several instances of people who have made false claims to membership of social groups such as military groups or the medical profession. For example, there is F.W.Demara who claimed (among other things) to be a doctor and professor of psychology. While Demara had no legitimate claim to being a doctor or a psychology professor, he was treated, and expected to be treated, as such because of his assertions that he was a member of these

social groups (and his ability to persuade others to believe him). In some cases, the claims made by criminals to be a member of a social group are sincere. They truly believe they are entitled to be a member of a particular social group despite not being eligible to join. An example is Treva Throneberry, a 31 year old woman who spent her twenties claiming to be a teenager, attending high school and using the foster care system (see chapter 6 for more).

As with social identity theory, self categorisation theory is important when considering identity related crime. Just as identity thieves will steal identities in order to gain access to social groups and exclusion from other social groups, they can – and do – go a step further and misrepresent the victim by asserting membership to social groups.

Confirmation of social group membership and identity

Social identity theory and self categorisation theory both emphasise the role of individuals in forming and choosing their own identity, but individuals need their claim to an identity confirmed by others within society and the social group they claim membership of. Without the confirmation and acceptance of the group any individual's claim to an identity will not be successful, regardless of the individual's opinion or belief in their identity. Identity is a construct which aids the social group, community and/or society in structuring and organising individuals' determining role and status within the group. Social role and status is discussed later in this chapter.

It is rare that society in its entirety comes together to identify an individual. More commonly, society is represented by representative groups who surround the individual as they seek identification. For example, a student who seeks to assert their identity in a class full of other students is dependent on the other students and the teacher acknowledging their claim to a particular identity. In this context, society is the other people in the classroom. There is interplay between an individual seeking to assert an identity and a group of individuals who represent society acknowledging or rejecting that individual's claim to identity.

It can be argued that in normal circumstance, society or an aspect of it is in control of the process of identification, but in cases of identity theft and fraud this relationship is undermined. It can also be argued that society's power to validate identity is dependent not only on the truthfulness of individuals but also trust that people will not subvert society's judgement. The threat that identity related crime poses to society is that it negates the power society has to confirm identity.

Forming bonds of trust, familiarity and solidarity

The use of trust in general is an important element in society, according to Newton (2007: 342):

> "The idea that trust is essential for social, economic, and political life is very old one going back at least to Confucius who suggested that trust, weapons, and food are essentials of governments: food, because well – fed citizens are less likely to make trouble, trust because in the absence of food, citizens are likely to believe that their leaders are working on the problem, and weapons in case neither of the other two work." (Newton .K, 2007: 342)

It is important to discuss trust in a study of identity related crime, as the abuse experienced in an instance of identity fraud is an abuse of a bond of trust. Bonds of trust can be found in many, if not all, identification processes and are not dependent on a prolonged or close relationship between the individuals involved. While people often form personal bonds of trust and relationships with family and friends, it can also be argued that they form bonds of trust with people they do not know in society, and that this capacity to extend trust to strangers is crucial for the maintenance of social order.

We trust people to conform to social contracts which dictate acceptable behaviour; we also trust people to acknowledge our rights and entitlements. Several studies have been conducted on how bonds of trust are formed. Deutsch (1958; 1960 cited in Ziller 1973) conducted studies into trust and bonds of trust. According to Ziller (1973), Deutsch defined trust as:

"....occurring in a situation where the individual is dependent upon the behaviour of another person in order to realize an outcome. He trusts the other person if he behaves in a way which renders him vulnerable to exploitation by the other, yet permits the other to act in such a way that both parties will benefit equally"
(Ziller .R.C, 1973: 41)

Hardin (1998) also argues that trust is a phenomenon based upon incentive, with people forming bonds of trust based upon self-interest and knowledge of other people's self-interest. Take the example of an interaction between a cashier at a bank and a customer depositing money. The customer will trust the cashier with their bank account details and their money because they have determined that it is in the cashier's interest to carry out the transaction. Hardin also argues that we do not trust people generally, and that trust occurs only in specific exchanges. Returning to the example of cashier and customer – according to Hardin the customer will trust the cashier in the specific situation of depositing money into the bank, but not in every situation in which they interact. This is because the depositor has some understanding of the institution of banking and the clerk has a specific role within that structure.

Hardin's view of trust has been criticised in Rothstein's study *Trust, Social Dilemmas and Collective Memories* (2000). Rothstein notes that Hardin's view of trust places a great deal of emphasis on the assumption that the person who is trusting is fully aware that it is in the interest of the person they trust to fulfil their request. Rothstein argues that according to Hardin's view of trust, as soon as it is not in the interest of the person being trusted to fulfil the request of the person doing the trusting, they will betray them. For instance, if we take the example of the cashier and the customer: Hardin's view of trust requires that the customer be fully aware that it is in the cashier's interest to fulfil the customer's requests. Furthermore, once it is not in the cashier's interest to fulfil the customer's requests, Hardin's theory argues that the cashier will betray the customer. Rothstein argues that in reality people could not and would not conduct complex calculations with regard to the self-interest of others. Rothstein further argues against

the idea that once it is no longer in the self-interest of someone to be trusted, they would exploit or abuse someone who trusts them. If, as Hardin argues, people would exploit each other once it was in their self-interest to do so, Rothstein claims this would make the practice of trusting a rarer phenomenon than it is in reality. People would not risk putting themselves at risk from shifts in others self-interests if, as Hardin argues, people will exploit or abuse them. The element of deception on the part of people who are being trusted further complicates Hardin's view of trust. Hardin argues that people who trust others must calculate the self-interest of the people they want to trust, but this does not take into account people who deceive people as to their genuine self-interest. Rothstein concludes that Hardin's view of trust as being about investment in others is problematic, as it will lessen the likelihood of people using trust. Rothstein refers to Granovetter's comment on trust:

> "a perception of others that one's interest in them is mainly a matter of 'investment' will make this investment less likely to pay off; we are all on the lookout for those who only want to use us" (Granovetter 1988 cited in Rothstein .B, 2000: 7)

The idea that trust is about self-interest and people's ability to discern the self-interest of others gives some insight into why certain bonds of trust are made within society. Bank loan agreements are an instance where both parties – the loan applicant and the bank – have determined that it is in their best interest to help each other, based on their understanding of what their self-interests are. The problem here is that the bond of trust is based on an accurate view of both parties self-interest. As Rothstein argues, it is open to debate as to whether or not people actually engage in an in-depth analysis of others' self-interests. Certainly, looking at bonds of trust formed between organisations and individuals, these can involve very little need for in-depth analysis of self-interest, there being only a general presumption of what individuals' self-interests are.

Luhmann (1988) also discusses the use of trust in society, in: '*Familiarity, Confidence, Trust: Problems and Alternatives*'(1988). Luhmann distinguishes between trust, familiarity and confidence, arguing that the concept of trust is roughly the equivalent to the idea of social solidarity. Luhmann argues that in the study of trust there is the potential to confuse trust with the concept of familiarity. According to Luhmann the concept of familiarity is useful as it explains the close bonds of trust which can exist between family members:

> "Familiarity is an unavoidable fact of life; trust is a solution for specific problems of risk. But trust has to be achieved within a familiar world, and changes may occur in the familiar features of the world which will have an impact on the possibility of developing trust in human relations. Hence we cannot neglect the conditions of familiarity and its limits when we set out to explore the conditions of trust." (Luhmann .N, 1988: 95)

As well as discussing the links between familiarity and trust, Luhmann also argues that trust and confidence are connected phenomena. Confidence and trust are used in situations where there is risk of disappointment and people will have expectations of a particular outcome. By trusting others, or having confidence in people, we place ourselves at risk of exploitation, but by not trusting others we place limits on what we as individuals can achieve or gain access to. The nature and level of trust we place in people can vary; who we trust and why can be a difficult thing to establish. It can be argued that in cases of identity related crime, familiarity, trust and confidence are all capable of being exploited and manipulated as in instances of identity theft and fraud. There are cases of identity theft that have exploited personal and close relationships where familiarity has played an important role. Certain cases of identity theft have occurred between family members where the familiarity between victim and identity thief has enabled the abuse of the victim's identity. Identity theft and fraud between family members is discussed in more detail in chapter 8.

In modern cases of identity theft there is often exploitation between people where there is no personal relationship, simply a transaction between an individual and a social institution. This requires a bond of trust between strangers. Trust in strangers is sometimes referred to as social trust. The concept of social trust is important to the study of identity fraud as often instances of identity fraud involve abuse of social trust. Social trust is defined as:

> "...a belief in the honesty, integrity and reliability of others – a 'faith in people.' It's a simple enough concept to describe. But it's never been easy to figure out who trusts, or why." (Taylor .P et al 2006: 1)

Social trust forms the basis for many interactions between individuals. One view of social trust is that it is trust in people with whom there is no personal relationship or familiarity to rely on. In other words social trust, 'trust in strangers', is a reliance on people (whom we do not know personally) to follow society's laws and social norms, and to be truthful. According to O'Neil (2002):

> "Each of us and every profession and every institution needs trust. We need it because we have to be able to rely on others acting as they say that they will, and because we need others to accept that we will act as we say we will. The sociologist Niklas Luhmann was right that 'A complete absence of trust would prevent {one} even getting up in the morning.'" (O'Neil .O, 2002: 3-4)

Social trust is an important concept in the study of identity theft and fraud as it is this bond of trust which is most often broken by criminals who assume false identities or the identities of others. It can be argued that without a system of trust between individuals, identity thieves could not operate; they exploit and rely on people's need to trust each other. In a study of social trust, Pew Research conducted a telephone survey of 2,000 adults who were asked questions to determine who were the most trusting people in America (Taylor et al, 2006). The study found that in America, white people were more trusting than black people or Hispanic people; people with higher family incomes were

more trusting than people from low-income families; married people were more trusting than single people; the middle aged and elderly were more trusting than the young; and those who live in rural areas were more trusting than those in urban areas. Pew's research also found in their research that issues of politics and religion played no significant role in influencing people's sense of social trust. On the issue whether or not other people could be trusted Pew's survey found that when asked the question, 'Generally speaking, would you say that most people can be trusted or that you can't be too careful in dealing with people?', (Taylor et al, 2006) 45% of respondents thought that most people are trustworthy, while 50% thought that you cannot be too careful in dealing with people.

While these statistics may imply that the people researched are almost evenly split between trusting and not trusting, it is worth noting that the people who participated in this study had enough social trust in the researchers to share their views with them. The extent to which people in the study really trust others, and whom they choose to trust is hard to determine; how would the research subjects react outside the context of the study when confronted with situations which require trust between individuals? In several cases of identity related crime, the talent of identity thieves in gaining the trust of their victims has been the key to convincing the victims that they can safely share information with them (see chapter 6). One area of society where social trust is of particular importance relates to commercial transactions. According to Arrow (cited in Huang 2003) in *Social Trust, Cooperation, and Human Capital:*

> "Virtually every commercial transaction has within itself an element of trust, certainly any transactions conducted over a period of time. It can be plausibly argued that much of the economic backwardness in the world can be explained by the lack of mutual confidence" (Arrow, 1972 cited in Huang .F, 2003: 1 – 2)

It can be argued that the U.K. and western society in general is dependent on a system of social trust in order to ensure that society can function. Arguably, a society without social trust would instead rely on lengthy process of confirmation, or be dependent on the formation of more personal bonds of trust. Given the complexity of modern society (in the U.K. and globally) it is unlikely that this could work effectively.

The concepts of trust, and specifically that of social trust, are important in the study of fraud as it can be argued that the only way fraudsters can succeed is if they are able to abuse some bond of trust. Sociological concepts such as role, status and self categorisation all come into play in an instance of identity fraud. An identity fraudster's ability and need to abuse social trust can be seen in the famous deception of Wilhelm Voigt 1906 who was able to steal 4,000 marks from the Mayor of Kopenick in Germany simply by pretending to be a captain in the Prussian Guards. Voigt was a petty thief who bought a second-hand Prussian officer uniform; he would put on the uniform and walk around Berlin, where he discovered that soldiers who saw him in uniform would snap to attention and treat him as a superior. According to Burton (2000) after realising that soldiers and people would react to him in his uniform as though he were a genuine captain in the Prussian Guard, Voigt decided to take his impersonation to the next step.

On October 17th 1906 Voigt entered a barracks and ordered a squad of soldiers to follow him to Kopenick so that they could arrest the mayor, who Voigt claimed had defrauded the state of 4,000 marks. Upon reaching Kopenick, Voigt had the mayor and treasurer arrested, and confiscated the sum of 4,000 marks and documents from Kopenick. Voigt sent the mayor and treasurer on the train to Berlin with an armed guard while he made off with the 4,000 marks. Voigt's actions sparked much controversy, with some objecting to his actions and others, including the Kaiser, seeing Voigt's deception as amusing. Voigt was captured several weeks after his deception and sentenced to four years in prison; however in 1908 the Kaiser decided to pardon Voigt. The case of the 'captain of Kopenick' was later turned into a play by Carl Zuckmayer which became very popular in German during the early 1930s as a story of resistance, humour and wit in the time of Kaiser Wilhelm (Ulbricht, 2006).

Voigt's deception is an important example of how identity fraudsters abuse social trust. Voigt needed very little to convince people he was a soldier, apart from his uniform and demeanour. If at any point anyone had questioned the role, status or self categorising of Voigt, they would have found out that he was not who he claimed to be. But in reality no one questioned Voigt; the soldiers he commanded never asked if he was a captain neither did the Mayor of Kopenick. The reason they did not ask can be attributed to their assumption of social trust between them selves and Voigt. They assumed that only someone entitled to take on the role of a captain would wear the uniform. Their trust was placed not in the man, but in the role he assumed and in the belief that only someone entitled to wear the uniform would do so. Howard (2008) also notes that:

> "Voigt exposed the fact that the soldiers had been so indoctrinated into following orders, and civilians had been taught such a reverence for a uniform, that anything could happen." (Howard .J, 2008: 2)

The exploits of Voigt and other identity thieves provide an insight into the abuse not only of social trust and solidarity but also the pursuit of self-interest and happiness. These concepts are discussed by both Emile Durkheim in *The Division of Labour* (1964) in the theory that modern society relies on social solidarity; and Utilitarian thinkers such as John Stuart Mill in his book *Utilitarianism* (1863), and his theorising on the individuals and societies pursuit of happiness. These theoretical perspectives place the discussion of trust between individuals, happiness and self-interest in wider theoretical discourses on the formation of social order.

Durkheim argued that a distinction can be made between traditional societies and modern societies. He argued that in modern societies an organic social solidarity forms between individuals, with people relying on each other to perform specialized roles in order to achieve social order. This interdependency means that people need to trust each other; hence the basis of social order in modern society is social trust. Without social trust how could society gain any kind of cohesion or social order?

In the context of a study of identity theft and fraud Durkheim's theories on social solidarity in modern societies goes some way to explain how identity thieves can succeed at their crimes. Victims of identity related crime can be seen as those who presume the existence of social solidarity between themselves and the identity thieves who victimise them. Rather than evaluating self-interest in others as Hardin (1998) describes trust, it can be argued that society and victims of identity related crime in particular adhere more to Durkheim's practice of social solidarity. An example would be people who are the victims of advance fee frauds such as phishing emails or Nigerian 419 scams (see chapters 6 and 7 for details). In these scams victims are lead to believe that they are entering into a legitimate interaction with the fraudster, assuming that the fraudster will adhere to the laws and social norms of society. Assuming this perspective is accurate, it can be argued that identity thieves exploit not only individual's trust in them but also by abusing social solidarity they undermine social order within society.

When looking at the motivation of identity thieves it is also worth considering the Utilitarian perspective on self-interest and the pursuit of happiness. The idea that people are rational individuals who place the pursuit of happiness and self-interest first explains in part why someone might engage in identity related crime. Identity thieves in this context are people who do not limit themselves and their desires to society's conventions and rules. The exploits of Voigt the 'captain of Kopenick' in the context of Durkheim's view of society and trust, can be seen as disruptive and an abuse of others. However from a Utilitarian perspective Voigt can be seen as someone who sought to achieve happiness by placing his own self-interest before any social solidarity he might have felt with his victims. His calculation, which proved to be mistaken, was that he would be able to carry out his act without any negative consequence. In accordance with Hardin's view of the formation of trust, identity thieves can be portrayed as people who not only pursue happiness and self-interest above and beyond any obligation to social solidarity, they are also people who assess the self-interests of others and use it to exploit them. Looking at the formulation of phishing emails and Nigerian 419 letters, the wording of these documents often seeks to attract people based on a calculating understanding of what victims find attractive (e.g. money, rise in social status).

As stated earlier these broader theoretical perspectives highlight the possible role social solidarity might have in people's susceptibility to identity related crime and the underlying motivations of identity thieves in pursuing self-interest above and beyond any social conventions others might follow. Voigt's exploits also highlight the importance of social symbols and the presumption of a person's role in society. Arguably, in the case of 'the Captain of Kopenick' the soldiers who followed Voigt substituted social trust and reliance on social symbols and the role Voigt took on for their own evaluation of Voigt's identity.

Roles and symbols

The concept of roles is discussed by George H. Mead in his 1934 book *'Mind, Self and Society'*. Mead argued that roles are a collection of social attributes and expectations associated with a social position. Roles are separated from an individual's character or personality and enable people to generalise over the behaviour of people in certain roles. According to Abercrombie, Hill and Turner (1984) roles are an important sociological concept:

> "Role is sociologically important because it demonstrates how individual activity is socially influenced and thus follows regular patterns. Sociologists use roles as the units from which social institutions are constructed. For example, the school as a social institution may be analysed as a collection of teacher and pupils which are common across all schools." (Abercrombie .N, Hill .S, Turner .B.S, 1988: 209)

In the context of identification, social symbols refer to any kind of badge or marker which identifies someone as being a member of a particular social group. Symbols can be a person's manner of dress, adoption of mannerisms or even their language or use of slang. Woodward argues that it is important for people to show their membership of certain groups and to distinguish themselves from members of another group. According to Woodward:

"...although as individuals we have to take up identities actively, those identities are necessarily the product of the society in which we live and our relationship with others. Identity provides a link between individuals and the world in which we live. Identity combines how I see myself and how others see me. Identity involves the internal and the subjective, and the external. It is a socially recognised position, recognised by others, not just by me." (Woodward. K. 2000: 7)

Social symbols are a way for individuals to assert their sense of self as well as their membership of social groups. By using social symbols, individuals can make it easier and quicker for others to identify them. For example, the use of uniforms and badges by the police enables people to identify police officers quickly and helps to assert that police officer's role in society.

The goal in displaying social symbols in an interaction between individuals is to establish who is responsible for what and what treatment individuals should expect. With the introduction of the National Identity Card Scheme, the government is seeking to introduce a specific highly individualised social symbol. The identity card is intended as a means of enabling people to display their status as U.K. citizens and their eligibility to various services and rights. The value of the identity card scheme is in part based on its ability to serve as a universal proof of identity, which would make it a powerful social symbol. If the identity card proves to be a popular social symbol of identity and citizenship this could have the knock on effect of making counterfeiting of identity cards more popular. If people rely heavily on the identity card as a social symbol, then its value to criminals increases. This issue will be discussed in more detail in chapter 9.

It is also through social symbols and the adoption of certain roles in society that social status is determined. Looking at the history of identity fraud, it is possible to highlight several famous cases of identity fraud where the individual in question sought to attain social status through the use of social symbols and the adoption of certain roles. An

example of someone who misused social symbols in order to attain role and status is Gene Morrison. Morrison was jailed for five years in 2008, after being found guilty of obtaining a money transfer by deception, obtaining property by deception, perverting the course of justice, and perjury. Morrison was found guilty of these crimes after it was discovered that he had spent over 26 years pretending to be a forensic psychologist and had provided forensic evidence in approximately 700 cases (BBC News, 2007).

According to Smyth (2007) Morrison did not lie about his name but he obtained a BSc degree Forensic Science, a Masters in Forensic investigation, and a Doctorate in Criminology from a fictitious American University. It was through the use of these documents – as social symbols – that Morrison was able to take on the role of a forensic psychologist. In this role Morrison was afforded the status of an expert in legal cases; his opinions and evidence were seen as being credible and reliable and influenced the outcome of criminal cases. In reality, Morrison had no skills in forensic science, and managed to keep up the pretence by subcontracting the work he was given to other forensic scientists and then passing it off as his own.

In terms of social role and symbolism, Morrison often used symbols such as his academic qualifications to claim ownership of the role of an expert in forensic psychology. For 26 years, Morrison effectively collected and used social symbols associated with what people would expect from a forensic psychologist. As well as the qualifications Morrison obtained, he also established his own business (Criminal and Forensic Investigations Bureau) and publicised his expertise in professional journals. Morrison's deceptions were not based on the use of another person's identity or on abandoning his own identity; he kept his name, but through a manipulation of social symbols was able to adopt a role in society that he was not entitled to. Morrison's case illustrates the trust people place in strangers, and their reliance on social trust.

Changes to society and their effect on identities

As discussed above there are many ways to view a person's personal or social identity and how it is constructed. Another important issue with regard to the discussion of identity is the effect changes in society have on the development of an identity. Issues

such as globalisation and the increased importance given to individuality have affected the construction and scope of people's identities. According to Ulrich Beck (2002), Western societies have developed so that people now strive to lead 'a life of your own':

> "We live in an age in which the social order of the national state, class, ethnicity and the traditional family is in decline. The ethic of individual self fulfilment and achievement is the most current in modern society. The choosing, deciding, shaping human being who aspires to be the author of his or her own life, the creator of an individual identity, is the central character of our time. It is the fundamental cause behind changes in the family and the global gender revolution in relation to work and politics." (Beck .U, Beck-Gernsheim .E, 2001: 23)

Beck's argument that western society has developed to be more individualistic in part is due to the breakdown of traditional bonds based on kinship, gender, social class and religion. The influence of modern of society on individuals' efforts to identify themselves is also discussed by Giddens (1991) in his book *Modernity and Self Identity*. In this book Giddens discusses what he terms the reflexive project of self. According to Giddens, individuals are actively involved in forming their own identity over the span of their life. Giddens' view of how an individuals formulate and revise their own identity is that this is effected through the use of biographical narratives. As Giddens notes, a biographical narrative is the story of who someone is and how they have developed. The process of forming a biographical narrative, according to Giddens, is something people do reflexively and a person's biographical narrative is consistently developed. Giddens also notes that it is possible for a person to have several different biographical narratives. In this way, a person can have or be developing several different aspects of their identity. Giddens argues that this is a result of post modernity:

> "What to do?' How to act? Who to be? These are focal questions for everyone living in circumstances of late modernity – and ones which, on some level or another, all of us answer, either discursively or through day-to-day social behaviour." (Giddens. A. 1991: 70)

Giddens discusses this issue in the context of the importance of self analysis in therapy. With reference to Rainwater's (1989) book *Self Therapy* Giddens suggests that the only way therapy can be effective is when patients become reflexive on the process and begin self therapy. Self-identity and the formation of a person's sense of self is dependent on individuals being reflexive and responsible for the creation of their own identity:

> "... what the individual becomes is dependent on the reconstructive endeavours in which she or he engages. These are far more than just 'getting to know oneself' better: self-understanding is subordinated to the more inclusive and fundamental aim of building/rebuilding a coherent and rewarding sense of identity." (Giddens .A, 1991: 75)

The process of developing and generating an identity is also linked to the adoption of a lifestyle. Giddens argues that one aspect of post modernity is that social roles are no longer assigned by society. In modern societies, people must choose to adopt a 'lifestyle', rather than being assigned social roles. The term lifestyle refers to a form of template that individuals can adopt to help form their personal identity and sense of self:

> "... in conditions of high modernity, we all not only follow lifestyles, but in an important sense are forced to do so – we have no choice but to choose. A lifestyle can be defined as a more or less integrated set of practices which an individual embraces, not only because such practices fulfil utilitarian needs, but because they give material form to a particular narrative of self-identity." (Giddens .A, 1991: 81)

Applying Giddens' views on reflexive project of self and lifestyles to the study of identity related crime is important. The activities of identity thieves are in a sense an effort to rebuild their self-identity by adopting aspects of other people's identities; taking control of who they are and how they will be perceived by others. This practice is a rejection of any control or influence society might have on the individual's self-

identity. The activities of identity thieves such as Arthur Orton, F.W. Demara and Charles Stopford (see chapter 6 and page 115 for details) can thus be seen as efforts to rebuild their identities and adopt lifestyles they were not entitled to. It can be argued that identity thieves, and these particular identity thieves display a great deal of reflexivity in the use of the identities they stole. Arguably, identity thieves are people who have a great understanding of how identities are formed and how to manipulate relationships of trust. The response of society to the discovery of Orton's, Demara's and Stopford's deceptions was to be scandalised as the three appeared to have rejected the power of society to dictate an individual's identity. According to Giddens, this is the reality of modern society; society has lost its role in determining self-identity.

It can be argued that this shift described by Beck and Giddens is due in part to the development of technology that allows for easier movement and communication. Changes in the means and amount of travel and communicating we do as individuals have allowed for more self expression. A by-product of this is the increased use of individuals' identities and a decrease in the importance of society or the community in establishing identity. This has caused an increase in the potential for identity theft and fraud. In the last ten years the development of the internet has created a new and unique venue for self expression. Online communities have formed, allowing people to express themselves and develop online versions of their identities:

> "Within a decade, the majority of North Americans will be living a Web Lifestyle." (Gates .B cited in Feather .F, 2007: 1)

It could be argued that Gates' predictions have come true, with websites such as MySpace, Facebook and Bebo providing people with a medium for self expression. The internet also provides commerce and a source of information about the world we live in. Commentators on the development of technology in the 21st century have argued that through the development of the internet and mobile phone technology society has gone through what Frank Feather (2008) calls a 'weboloution' (internet revolution). Dr William Webb an expert in mobile communication speculates that in the future mobile

phones will be in effect a 'remote control' for our lives. Mobile phones will inform, entertain and plan out our daily lives providing constant access to a various pieces of information provided on the internet.

Globalisation

The development and increased use of the internet can be seen as an element of the movement towards globalisation. Globalisation is defined by the World Bank Group (2007) as the integration of different nations' economies and societies. A briefing paper for the World Bank Group by PREM Economic Policy Group and Development Economics Group (2007) discusses some of the difficulties in explaining the term globalisation:

> "Amazingly for such an extensively-used term as globalisation, there does not appear to be any precise, widely-agreed definition. Indeed the breadth of meaning attached to it seems to be increasing rather than narrowing over time, taking on cultural, political and other connotations in addition to the economic. However, the most common or core sense of economic globalisation – the aspect this paper concentrates on refers to the observation that in recent years a quickly rising share of economic activity in the world seems to be taking place between people who live in different countries." (PREM Economic Policy Group and Development Economics Group, 2007: 1)

Work by sociologists, such as Ulrich Beck's (2000) *What is Globalisation?*, Hazel Henderson's (1999) *Beyond Globalisation*, and Robert J. Holton's (1998) *Globalisation and the Nation-State*, illustrates how in the later part of the 20th century the phenomenon of globalisation has arisen. This has lead to the formation of companies and organisations which transcend nation states, increased sharing of cultural ideas and concepts, and increased communication between people in different countries. With regard to the study of identity and identity fraud the increase in communication between people in different countries is of particular importance as identity related crime can be

committed over the internet and involve criminals in one country victimising people in another. It also minimises the amount of time taken to set up and commit identity fraud.

The role of the internet not only as a means of communication but also as an extension of the system of social trust may or may not be a good thing. O'Neil (2002) notes in her book *A Question of Trust* that perhaps the internet is both a good and bad thing in terms of the formation of bonds of trust:

> "Perhaps we are in luck. We live in an age of communication technologies. It should be easier than it used to be to check out strangers and institutions, to test credentials, to authenticate sources and to place trust well. But unfortunately many of the new ways of communicating don't offer adequate, let alone easy, ways of doing so. The new information technologies are ideal for spreading reliable information, but they dislocate our ordinary ways of judging one another's claims and deciding where to place our trust." (O'Neil .O, 2002: 84)

It can be argued that the development of lines of communication with people on a global scale means that there is often an element of risk and uncertainty to the relationships formed. O'Neil's (2002) argument, that we cannot rely on ordinary or traditional methods of judging trustworthiness, means that when we do form bonds of trust over the internet we are taking a risk. Issues of risk and uncertainty are discussed by Beck (2001) in his book *Individualisation*; according to Beck:

> "The narrative of risk is a narrative of irony. This narrative deals with the involuntary satire, the optimistic futility, with which the highly developed institutions of modern society - science, state, business and military - attempt to anticipate what cannot be anticipated. Socrates has left us to make sense of the puzzling sentence: I know, that I know nothing. The fatal irony, into which scientific-technical society plunges us is, as a consequence of its perfection, much more radical: We don't know, what it is we don't know - but from this dangers arise, which threaten mankind!" (Beck .U, Beck-Gernsheim .E, 2001: 1)

On the issues of identity theft and fraud and the identity card scheme, there is often discussion of risk and preventing dangers. Advice given by organisations such as the Credit Industry Fraud Avoidance System (CIFAS) often emphasises minimising risks posed by identity thieves through data security measures such as shredding documents before discarding them. The arguments posed by opposition groups against the identity card scheme often refer to the risks posed by giving the government too much power. Phrases such as 'surveillance society' and 'database society' refer to the danger of too much monitoring of citizens' movement and control of the identification processes. In both contexts, the emphasis is on addressing known risks and perceived dangers. This situation, as Beck argues, still leaves us unable to protect ourselves from threats we do not know about or are unable to anticipate. In terms of the threat posed by identity related crime, part of the perceived problem is that the general public are unaware of the risks posed by identity related crime and are unable to protect themselves against it. Take for example the experience of Derek Bond and the media attention his arrest received. What made his experiences in South Africa so shocking was that he had no idea his identity had been stolen and could not anticipate or prevent his arrest. Despite the media reporting of Bond's experience, it appears that people still face difficulty in anticipating or protecting themselves against identity related crime. According to the Identity Theft Resource Centre's 2008 survey of the effects of identity theft, victims of identity theft in America take on average 58 hours to clear up cases of account takeover.

Conclusion - broader issue of identity

The study of identity is a vast area of research in sociology, and presented here in this chapter is an overview of some key concepts that directly relate to the study of identity related crime. As mentioned earlier, concern over identification in the 21st century has increased. Attacks on the identification processes through terrorist activity, illegal immigration and identity theft have spurred movement on the re-introduction of the National Identity Card Scheme. Inherent in the discussion of both identity theft and identity cards are the themes of accurate identification and trust which are discussed in

social identity and social trust theory. The use and abuse of social symbols and roles are also an important aspect of the discussion of identity theft.

The concern over identification and security is furthermore a part of a larger concern over identity and an interest in studying the nature of identity. The study of identity has become an important issue in the U.K. in the last decade. Starting in 2004, the Economic and Social Research Council (ESRC) Identities Programme (2003) has funded the Identities and Social Action research programme, consisting of 25 studies into various aspects of identity over five years. The programme was established in order to investigate recent developments in the formation of identities. In the proposals for the programme it is argued that:

> "These are interesting times for the study of identity. Identity is central to many of the most significant developments in contemporary society. It has been suggested, for instance, that social and technological changes have led to the replacement of stable identities based on familiar social class hierarchies with multiple, fragmented and more uncertain identity projects based on 'life-style' and consumer choices. It has been argued that family and work-place loyalties and traditional political and community commitments are breaking down and have been replaced by a more volatile and dynamic 'identity politics'. Many have stressed the upsurge of intense solidarities based on religious, ethnic and national identities. The negative side of this is expressed through exclusion and through hostility towards those with different identities." (ESRC Identities Programme, 2003: 1)

Part of the justification for the Identities and Social Action Programme is that there are several theories on identity and identification which have received insufficient research and testing. Luhmann also argues that the study of trust has not been a central concern in the study of sociology, with both traditional theorists and modern thinkers failing to address the issue of trust. So while this study focuses on identity related crime, it is

important to note that it is part of a broader discussion of the nature of identity and the role of trust in society; aspects of which this study will touch upon.

CHAPTER 3

Fraud

Introduction

Fraud as a subject of criminological study has often been associated with the activities of certain social groups. Often the emphasis of criminology with regard to fraud has been on the individuals who use this type of criminal behaviour, rather than the crime itself. One of the developments with regard to fraud that this study will look at is the shift from focusing on the social groups who use fraud, to the specific study of fraud and its variations. It will be argued in this study that identity fraud as a concept is not a new type of crime but rather a change in the way criminology discusses and views fraudulent activity.

In order to review the literature on identity fraud, this chapter will look at four areas of criminological theory and discourse which deal with the crime of identity fraud and the people who are associated with its use. Firstly this chapter will look at academic studies of identity fraud from America, Australia and Britain and discuss the various different definitions of identity fraud that have developed. Secondly, this chapter will look at organised crime and its use of identity fraud as part of various criminal enterprises. The third part of this chapter will focus on the issue of the use of identity fraud in organised crime (people trafficking and illegal immigration), and will also cover Lord Grabner's report on the 'Hidden Economy'. In the final section of this chapter, the use of identity fraud by terrorists will be assessed.

Literature on identity fraud

The literature on identity fraud can be broken down into three main areas of research based on the work of criminologists in the three countries America, Australia and the U.K. From each of these countries there have developed different definitions of identity fraud and perspectives on the scope of the terms identity fraud and identity theft.

Identity theft – the American definition

Identity fraud is a crime that came to the public's attention in America during the mid to late 1990s due to high profile instances of identity theft (see the story of Michelle Brown on page 109). The term identity theft became popular for describing crimes which in the U.K. are often referred to as identity fraud. While both the terms identity fraud and identity theft are used in the U.S.A., it is argued by some that identity theft is a sub group/definition of identity fraud. The term identity theft is popular in U.S. legislation, media discussion and governmental reporting. In a report by the General Accounting Office (GAO) for the subcommittee on Crime, Terrorism and Homeland Security, and the subcommittee on Immigration, Border Security, and Claims, Committee on the Judiciary, House of Representatives, Richard M. Stana discusses identity fraud and its connection to identity theft:

> "…. 'Identity Fraud' – a term that encompasses a broad range of illegal activities based on fraudulent use of identifying information of a real person or of a fictitious person. A pervasive type of identity fraud is identity theft, which involves 'stealing' another person's personal identifying information – such as Social Security number {SSN}, date of birth, and mother's maiden name – and then using the information to fraudulently establish credit, run up debt, take over existing financial accounts, or to undertake other activities in another's name. Also, another pervasive category is the use of fraudulent identity documents by aliens to enter the United States illegally to obtain employment and other benefits. The events of September 11, 2001, have heightened concerns about the contributory role that identity fraud plays in facilitating terrorism and other serious crimes." (Stana .R.M, 2002: 2)

Academic study of the subject of identity theft and identity fraud in America has provided several definitions of the two terms. According to Newman and McNally (2005):

> "Identity theft is rarely one crime, but is composed of the commission of a wide variety of other crimes, many if not all of which are crimes well known to us all. The crimes with which identity theft is commonly associated are: check and card fraud, financial crimes of various sorts, various telemarketing and Internet scams {Newman and Clarks 2003}, theft of autos and auto parts aided by fraudulent documentation {Maxfield and Clake 2004}, thefts or robberies of various kinds where identification information is stolen either by coincidence or intentionally, counterfeiting and forgery, trafficking in human beings {UNICRI 2003} and terrorism." (Newman .G, McNally .M.M, 2005: 2)

In their report for the Department of Justice, Newman and McNally outline the several different types of identity theft that exist in the U.S.A.:

U.S definitions of identity theft by Newman and McNally (2005)

1. Exploiting Weakness in Specific Technologies and Information Systems.
2. Financial Scams.
3. As a motive for other crimes.
4. Facilitating Other Crimes.
5. Avoiding Arrest.
6. Repeat Victimization: "Classic" Identity Theft.
7. Organized Identity Theft.

The definitions developed by Newman and McNally highlighted the ways in which identity can be abused in order to facilitate criminal activity. They acknowledge that while identity theft is not a new crime, the increased media profile of victims of identity theft and the development of technology has compelled the state to give this type of crime more attention. While the U.K.'s response to the problem of identity theft and

identity fraud was to propose the introduction of identity cards, the U.S. approach was to criminalise identity theft by introducing the Identity Theft Act of 1998 (discussed in chapter 8). The U.S. system of identification relies on the use of social security numbers and the use of drivers' licences with picture ID to establish identity which in effect is similar to the use of National Insurance numbers and drivers' licences in the U.K. When the idea of introducing an identity card was suggested after the September 11th 2001 terrorist attacks, the idea was dismissed as a solution to preventing future terrorist attacks in America.

Identity fraud in the U.K.

The crime of identity fraud has become a more acute problem for the U.K. since the millennium and several criminologists have researched and discussed the nature of identity fraud. In a report for the Department for Trade and Industry by Gareth Jones and Michael Levi (2000) the subject of identity fraud is comprehensively discussed and defined. In this report Jones and Levi argue that identity is an important aspect of social life in that it represents the need for trust between individuals. :

> "Society and commerce depend on trust, and assurance of identity is one important facet of that trust, though it simultaneously indicates distrust that people might not be who they claim to be. So that is, we believe, an important topic that goes beyond the creation or inhibition of economic crime opportunities – significant though that is in itself – and touches issues such as the sense of integrity of self, which is disturbed profoundly by impersonation." (Jones .G, Levi .M, 2000: 1)

Jones and Levi also note that with the emergence of the internet the need for face-to-face meeting is decreasing and this brings with it an increase in the need to identify ourselves to strangers. The work of Jones and Levi was carried out in 2000, and since then it can be argued that the use of the internet by individuals and organisations has increased. According to statistics on world usage of the internet formulated by Internet World Stats (2007), between the years 2000 and 2007 there has been a 265.6% increase

in the use of the internet. The reliance placed on the internet by private companies and state agencies has significantly increased, with many organisations providing online access for customers. The benefits of using the internet is that services can be provided quickly and in many instances through the use of an automated identification process which the customer can complete without the need for assistance from a member of staff. While, arguably, services provided over the internet are not the norm, the increased use of internet identification processes has had a significant impact on the way people interact and the way people commit identity fraud. Techniques such as phishing and pharming capitalise on the lack of face-to-face interactions. In some instances, the risk of fraud is such a concern that face-to-face identification is made mandatory to ensure accurate identification. Examples of this include adult applications for National Insurance numbers and applications for state benefits.

Also in Jones and Levi's study, the process of identification is discussed in detail as are the methods used to commit identity fraud. Jones and Levi outline the creation of a person's identity from birth to death and highlight the significant forms of identification that are obtained or adopted as a person grows up. They also outline the different ways a person can change their identity in the U.K.

Jones and Levi refer to two sociological classifications of a person's identity. The first is a person's *attributed identity* which refers to the identity given to someone at birth; this includes details such as name, date of birth and names of parents. The second is a person's *biographical identity*. A person's *biographical identity* refers to the identity that is formed by a person's interactions with other members of society. This form of identity is formed through interactions with others in both the public and private sectors of society. Jones and Levi go on to argue that while every individual in a society is given their own individual attributed identity, a person's biographical identity depends on their interactions with others.

They highlight the examples of children and immigrants who, while having *'attributed identities'* may have minimal *'biographical identities'* in the commercial sectors of U.K. society. For example, a child, while having a name and date of birth (attributed identity), may not be old enough to gain access to a bank account or develop a credit record and therefore will not have a significant biographical identity in the private sector. As a consequence of this, banks and credit companies will be unaware of the child's existence.

From this distinction in the classifications of identity Jones and Levi argue that the formation of an identity is not reliant on the attributed identity that is provided at birth; an identity can be formed on the events that take place in a person's life which go to form a person's biographical identity.

> "Traditionally, identities are compiled from the starting point - the birth certificate – but this is increasingly redundant. In a new age of greater interactions that are not face to face, with higher expectations of instantaneous responses for customer service, and new thinking on matters of establishing trust, the fact-on-computer usually characterised as 'data' is king and provides for significant personal and commercial advantages for those able to leverage them." (Jones .G, Levi .M, 2000: 4)

The process of identification in the U.K is, according Jones and Levi, a cumulative process.

> "Individuals accumulate evidence of identity – proof documents, and if the number and type of these proofs meets the required threshold, the individual is deemed identified." (Jones .G, Levi .M, 2000: 5)

The process described by Jones and Levi reflects some of the key themes discussed in sociological theories of identity. These concern the use of social symbols and labels in the form of proof documents, and the role of society in confirming the claims of

individuals. Jones and Levi also highlight the use of numerous forms of identification in ensuring accuracy in identification processes. They go on to argue that this is a risky way of establishing an identity as it leaves society open to identity fraud. With regard to fraud, Jones and Levi argue that there are five basic types of personal identity fraud and four types of commercial identity fraud. The typology discussed here by Jones and Levi is an important development in the study of identity fraud as it represents an early attempt to codify and distinguish different types of identity fraud. Fraud, in the context of the work by Jones and Levi, refers to instances of manipulating the identification process.

The first form of personal identity fraud discussed by Jones and Levi is termed *Current Address Impersonation*; here the Post Office's redirection service is used to divert a household's mail to another address in order to gain access to identifying documents and details from bills and bank forms delivered through the post. Jones and Levi distinguish between a variety of different types of current address impersonation. Their distinctions are based on the status of the householders. Jones and Levi distinguish between people who are residents at an address, people who have just left a residence or people who are on holiday or living abroad. Different types of householders will have different levels of awareness with regard to the activities of identity fraudsters using this approach. While a resident of a household may notice the sudden lack of mail, people who have just left a property may not be aware of fraudsters using this approach for some time, nor might people who have been absent from their residence because they are on holiday or living abroad.

The second form of personal identity fraud is *Previous Address Impersonation.* According to Jones and Levi there are two forms of previous address impersonation. The first form is where a fraudster will use the address history of another person with the same name as the fraudster. The fraudster will use the address history of the victim on application forms. The second type is where the fraudster will adopt a person's identity and make it appear that they have moved residence; the fraudsters will use stolen and forged documents to back up the claim that the victim has moved house.

The third type of personal identity fraud is where a fraudster adopts the identity of a dead person. Of this type of identity fraud impersonation of dead elderly people and dead children can be the most lucrative. Theft of the identities of people in other age groups does happen (see identity fraud during natural disasters in chapter 7); however, it can be argued that the theft of dead children and elderly people's identities can provide identity thieves with a greater chance of success and better chance of avoiding detection.

With the impersonation of dead elderly people, the fraudster establishes, through publicly available sources such as obituaries that an elderly person has died. According to Jones and Levi the identity of the dead elderly person is then used in conjunction with current or previous address impersonations to create a biography. In this type of personal identity fraud, it may be difficult to obtain official documentation as there may be an age gap between the fraudster and the victim.

The use of dead children's identities is another form of identity fraud. The appeal of this form of identity fraud for fraudsters is that these identities are not well established and therefore the identity can be established by fraudsters without the threat of discovery. In this form of identity fraud the birth certificate is very important:

> "The birth certificate is the turnkey or precursor to obtaining a passport, the passport can be used to support an application for a driving licence, and so on. The fraudster will invariably establish the identity in the commercial sector by opening up utility accounts, opening accounts for certain types of financial services and even take a driving test to obtain a 'full licence' in a false name." (Jones .G, Levi .M, 2000: 8)

This form of identity fraud is often very traumatic for the family members of the dead child if they are called on by the authorities. As with the current and previous address based identity fraud the potential for detection by the legitimate identity holder is a factor in this type of identity fraud. (see story of Charles Stopford page 115)

Another form of identity fraud discussed by Jones and Levi involves creating fictional identities that do not require the copying of a genuine identity. This type of identity fraud is achieved through abuse of official sources of identification such as the Driving Vehicle Licensing Agency. Other methods of developing an identity are through the use of documents that have no official or practical value as identification documents, such as utility bills. These documents do not identify the person presenting them as the genuine holder of the identity they only provide proof that the identity exists. According to Jones and Levi, this form of identity fraud is on the decline as the use of fraud prevention tactics and photo identification are increased.

The final type of identity fraud discussed by Jones and Levi is transactional impersonation. Transactional impersonations refer to fraudsters who use stolen identity documents and attempt to pass themselves off as the rightful bearer of the document. Examples of this are crimes such as credit card fraud and using stolen cheques. This type of identity fraud often involves the forging of signatures or the altering of documents such as cheques. Transactional impersonations also refer to the creation of counterfeit credit cards. According to Jones and Levi, there has been a growth in this type of identity fraud, often used by criminal organisations because of the ease with which cards with magnetic strips could be copied. They highlight the use of magnetic card readers by gangs of counterfeiters to 'clone' the credit details from victim's credit cards (This report was published before the introduction of chip and pin systems on various credit and debit cards).

As well as referring to financial transactions, transactional impersonations also refers to the use of counterfeit or forged identity documents in other contexts. The use of transactional impersonation can be seen in the impersonation of police officers through the use of fake warrant cards or the impersonation of utility workers by counterfeit work IDs.

As well as personal identity fraud there is also commercial identity fraud. Jones and Levi identify several types of commercial identity fraud:

> "There are several ways in which companies can be attacked, such as by surreptitiously registering new bogus Directors and by transferring the company's registered address, or copying its identity by loading fake web sites to the internet that look very similar to the genuine company's site, with the aim of collecting information about an individual and their payment card, with which to subsequently commit card not present fraud." (Jones .G, Levi .M, 2000: 9)

As well as defrauding companies, identity fraud can also be used in the purchasing of companies. Fraudsters can purchase companies under assumed names. While the company is genuine the directors or owners and their intentions for the company are not.

As well as classifying the different categories of identity fraud, Jones and Levi also look at the consequences of identity fraud. They highlight the problems faced by victims of identity fraud:

> "The true owner of the identity – who is invariably unaware of the iniquitous activity being committed in their name – has an administrative mess ahead of them to resolve. They have to disassociate themselves from the offence, clean their data records to reflect their non-involvement in the frauds and potentially erroneous default notices, and organise for the re-issue of documents and cards. They may have to provide witness statements to police, attend court proceedings, and this can go on for many months and even years. " (Jones .G, Levi .M, 2000: 10)

Jones and Levi argue that people's identities are under threat as a person's privileges, rights and rewards are connected to their identity and the identification process. The various forms of identification are also discussed by Jones and Levi who argue that there are a variety of defences against fraud around these processes. Within the different

processes of identification there is a need to test for validity and verification. The first step is to ensure the person exists and the second is to ensure that person presenting the identity is the true identity holder.

> "The modern thinking on identity is that two separate equations should be satisfied. The first is to show that the individual actually exists. The second is to show that the applicant is or is not the individual they say they are." (Jones .G, Levi .M, 2000: 11)

However, it is argued by Jones and Levi that there is no identification process that is completely safe from fraud. In the commercial sector, the reason for this is that there is more of an emphasis on speed than safety. This is due in part to the perception that a quick service is a good service. Advertisements for loan and credit companies emphasise their ability to provide 'quick and simple' application processes. Some companies even encourage people who may have problems obtaining a loan due to debt or county court judgements to apply for loans. This may be a cultural phenomenon that has developed due to the availability of technology which allows for quick communication over large distances. As stated earlier, statistics formulated by Internet World Stats (2007) on world usage of the internet have shown a significant increase. As well as seeing a rise in the number of people who use the internet, it is also important to note that, with regard to e-commerce, there is a perceived need to increase the usability of the internet. Usability is a term which refers to a trend towards making websites easy to use and accessible to as many people as possible. According to Nielsen (2003):

> "Usability is a quality attribute that assesses how easy user interfaces are to use. The word 'usability' also refers to methods for improving ease-of-use during the design process" (Nielsen .J, 2003: 1)

Usability is something that Nielsen argues everyone involved in the running of a web based business should seek to improve. Nielsen identifies five different aspects of usability : learnability, efficiency, memorability, errors, and satisfaction. Learnability

refers to how easy it is for people to learn how to use a website the first time they encounter it. Efficiency is how quickly visitors to the website can perform tasks. Memorability is how easy it is to remember how to use the website after a period of not using it. Errors refer to how many and how severe the mistakes people make when using the website are. The final aspect of usability is how satisfying the website is to use. Nielsen argues that maximising these elements of usability is important in any website design as it ensures customers will return to the website.

In terms of identity fraud, the perceived need to improve usability of websites can be seen as a detriment. It can be argued that by making it easier for people to use websites, they are also making it easier for identity thieves to operate. It can also be argued that the easier and the quicker it is for someone to conduct transactions on the internet, the easier it is to use a stolen identity.

This tendency to make the use of websites and companies on the internet easier and quicker can be seen as a continuing problem in society in general. Organisations are encouraged to make their services quicker and easier for their customers to use. The identification process in the U.K. is, according to Jones and Levi, ill-equipped to deter fraudsters. They argue that identity is established by the accumulation of paper proofs which have limited or inadequate security surrounding them. The security surrounding birth certificates, for instance, is non existent, as anyone can obtain a copy. With a birth certificate all manner of identifying documents can be obtained and an identity can be established. The lack of regularised notification of fraud risks to individuals surrounding certain documents is also determined to be a serious problem according to Jones and Levi, as there is an apparent rise in the levels of fraud in the U.K.

Since this study by Jones and Levi in 2000, the practice of warning people of threats to their identities has been taken up by some aspects of society. Often warnings for specific threats are issued, such as in the case of the eBay phishing attack of July 2003 – July 2004 where 160 customers of the online auction site had their details stolen. Aside from

this form of notification, there are also several websites which provide details on various threats people might face from identity fraudsters both on the internet and in general.

Alternatives to the current system of identification are also discussed by Jones and Levi, such as the efforts made by the information solutions company Experian to create a new identification process:

> "...Experian measures identity in a new way that harnesses credit scoring expertise to measure data evidence of life events, scores these for provenance and reliability – validity, and then tests all the data for consistency and fraud risks to provide for verification to reach a final identity score." (Jones .G, Levi .M, 2000: 14)

It is argued by Jones and Levi that the system proposed by Experian provides the ability to detect cases of identity fraud. Experian also provides a process that will quickly deal with legitimate and easily validated identities and provide an alternative process for identification where there is a degree of doubt surrounding the validity of the identity.

An alternative approach to the identification process reviewed by Jones and Levi is the use of 'challenge and response questioning'. This approach involves checks on information provided by the person entering the identification process with third party sources in the public and private sector. Once these initial checks are completed the individual is questioned on specific details that only the genuine identity holder should know. If the applicant is able to answer the questions then it is suggested by this approach that the individual is the valid holder of the identity. According to Jones and Levi, this approach runs into difficulty if the individual in question has had very little contact with the public or private sector.

Jones and Levi favour these new approaches as the process of identification is based on qualitative issues of validity and verification. This is in contrast to the current approach which favours a quantitative approach by relying on the reaching of a cumulative

threshold of paper proofs. Jones and Levi note that the only area that could not be covered by these new models of identification is where there is collusion between the individual committing identity fraud and the victim of the fraud.

As well as discussing identity fraud and the identification process, Jones and Levi also discuss the right to anonymity and the formation of trust without identity. Jones and Levi argue that the majority of commercial transactions are anonymous and there is no expectation on the part of individuals to have to identify themselves. However, it is through the identification process that trust is created between the individual and the service provider.

The future of the development of trust between individuals is an important area of discussion in this study. It is argued by Jones and Levi that future efforts to formulate trust may be formed on accumulated transaction patterns and performance. Rather than relying on identity formed from evidence of life events, trust and identity would be formed from a person's performance as a consumer. Jones and Levi do note that a possible downside to this approach is the devaluing of a person's identity if the performance in the context of financial transactions decreases.

This shift from a process of identification based on life events to performance as a consumer is in part used by the credit industry. Credit ratings are issued to individuals by credit providers and are used to determine a person's reliability when lending them money. A bad credit rating can result in someone being denied a mortgage, credit card or a loan. In some cases of identity fraud, the damage done by the identity thief has resulted in the victim receiving a bad credit rating. While the victim can be reimbursed for the money they lost in the instance of identity fraud, repairing a person's credit rating can be more difficult. In several cases of identity fraud, the real damage done to victims has been the decrease in their credit rating which they have had difficulty reinstating. Since 2003, concern over the abuse of a person's credit rating has been combated in 40 states in America in the form of fraud alerts and credit freezes. If a person in the U.S. believes they have been the victim of identity fraud, they can contact

a credit reference company such as Experian and issue a fraud alert notifying them of any attempt to open a new credit account. Aside from issuing a fraud alert, it is also possible to issue a credit freeze on a person's identity. A credit freeze prohibits any form of credit account from being opened, effectively shutting down that identity's ability to obtain credit. Since 2007 the credit industry in the U.K. has considered introducing credit freezes as a method of fraud prevention. By using credit ratings, it can be argued the credit industry has effectively reduced a person's identity to that of an account whose value is based entirely on their economic viability.

The process by which we confirm identity is an important factor in the study of identity fraud. While the use of alternative approaches such as credit ratings to determine identity may be gaining in popularity, the more conventional process of assessing identity by looking at life events is still common. This may be due to the continued efforts of individuals to formulate identity through the use of biographical narratives (as discussed by Giddens 1991 in chapter 2).

Jones and Levi also look at the role of technological innovations in confirming identity and influencing how identity fraud is committed. They discuss the impact of smart cards and biometrics, and the decrease in face-to-face interaction. Jones and Levi highlight the use of new technology and its impact on the formation of identity and outline the impact on crime control:

> "...if the criminal becomes aware that they can be identified more easily than ever before, how might this change their behaviour? If they recognise the risk, there could be two effects. They will either be displaced through target hardening into committing other crimes where the risk of being identified is less, or exercise leverage upon others to commit crimes for them, for example by kidnapping or blackmail. Identification might not cause them concern, if the short term gain is worth more to them than the ultimate sanction. The uplift to law enforcement would be more focussed investigations, and less opportunity for judicial error. " (Jones .G, Levi .M, 2000: 19)

In conclusion, it is noted by Jones and Levi that by introducing the identity card scheme, the government is attempting to introduce a new database which will define who actually exists, and then to ensure through biometric security measures that people cannot use another person's identity or create a fictitious identity. It is thought that by establishing and registering who exists and then preventing any alterations, identity fraud can be prevented. This approach, however, assumes that the true number of people living in the U.K. can be determined and that measures to ensure that people cannot alter or use other peoples' identities will be successful. These issues and others are the focus of this study.

This paper outlines the current state of identity fraud and the methods of committing this type of crime, as well as the possible future uses or changes to the identification process. Later, some of the changes discussed by Jones and Levi, such as biometrics and smart cards, will be discussed, as they have been introduced since this report was published. While the report by Jones and Levi outlines a very specific view of identity fraud, there is still room for looking at identity fraud in a wider context.

Since the work by Jones and Levi others have updated and re-conceptualised definitions of what constitutes identity theft and identity fraud. Work by Semmens (2006) and Finch (2003) provides newer definitions of identity fraud and identity theft and comment on the differing uses of the two terms. According to Semmens:

> "There are essentially two defining features of identity theft. First, there must be an 'appropriation' of another individual's personal data and, second, an act of 'impersonation' in which the perpetrator masquerades as that individual in order to commit another crime." (Semmens .N, 2006: 3)

Another definition of identity theft is provided by Finch (2003) who, rather than using the term identity fraud, focuses on the term identity theft and provides two methods or types of identity theft - *total* and *partial* identity theft. Total identity theft refers to the

assumption of another person's identity and the abandonment of the identity thief's identity. Other definitions of identity fraud and identity theft refer to this type of identity theft as wholesale assumption. The term partial identity theft refers to all types of identity theft that involve the short term abuse of a person's identity as a means of committing or enabling a criminal offence.

Aside from the definitions of identity fraud provided by criminologists there is also the definition provided by the Fraud Advisory Panel to consider. In their report on identity fraud 'Identity Theft: Do you know the signs?'(2003), identity fraud is separated into four different types:

- "Application Fraud – where a fraudster applies for payment cards and financial products in the name of his victim;
- Account take over – where the fraudster collates sufficient information about the victim to dupe the victim's bank that they are the victim;
- Wholesale assumption of the victim's identity – obtaining false passports and identification documents or using the identity of a dead person which may result in fraudulent claims for social security benefits;
- The fraudulent use of a business identity." (Fraud Advisory Panel, 2003: 1)

Burton (2000) provides an alternative view on the issue of identity fraud focusing on impersonation, and distinguishing between the different intentions behind people's impersonation and the length of their impersonations.

"...In attempting to categorize different kinds of impostors, however, there is one simple and useful division into two broad but distinct types. The first category consists of those people who use imposture to gain what could never rightfully be theirs. They may pose, for example, as an heir to an estate, or as some remarkable person in order to gain fame and fortune. Whereas this group use imposture in order to pretend to some great achievement or status, the second

group use imposture to enable them to achieve. This group comprises genuinely and prodigiously talented people who, in their 'real' lives, would never have the opportunity to exploit their abilities and intelligence. The first group pretend they have achieved {or inherited}; the second group pretend in order to achieve. They could be called, respectively, opportunists and pragmatists." (Burton .S, 2000: 4)

While the issues presented in the U.K. definitions mirror many of the concerns presented in the U.S. definition, it can be argued that the timing of the rise in concern over identity fraud has played a greater role in the levels of concern over identity fraud in the U.K. than in America. While identity fraud has been an issue in America since the 1990s, the rise in concern over identity fraud in the U.K. came during the rise in concern over illegal immigration and terrorism at the beginning of the 21st century. In the last eight years of the 21st century, stories about terrorism, illegal immigration and large scale cases of identity fraud have received a great deal of media attention.

While the threat of identity fraud faced by America and Australia has, in many respects been the same as that faced in the U.K., what makes the U.K. experience of identity fraud unique is the time frame in which public awareness was increased. The idea that identity fraud is a new 21st century crime is due in part to the way identity fraud has been introduced to the U.K.

The work by Jones and Levi (2000), Finch (2003), the Fraud Advisory Panel (2003) and Semmens (2006), represents some of the most recent commentary on identity fraud. It is apparent that changes in the way people interact, in particular the use of the internet have raised issues concerning the formation of trust between individuals. Identity fraud as a subject deals as much with criminal opportunity surrounding the identification process as it does with individual types of crime, such as credit card fraud or illegal immigration.

Another aspect of the study of fraud is the manner in which it is investigated and the emphasis placed on stopping this type of crime. In an article by Michael Levi on the Roskill Fraud Commission (2003), Levi discusses the commission and the allocation of resources and attention to fraud and associated crimes. Levi criticises the current approach for undermining the importance of investigating fraud. According to Levi there is little political pressure to tackle fraud; this is due in part to the difficulty in distinguishing many types of fraud from legitimate financial practices. However the lack of interest is not limited to people in charge of policy, and Levi notes that:

> "Only in the City of London is policing fraud a key local police objective." (Levi .M, 2003: 38)

Levi later mentions that:

> "In the study for the National Fraud Working Group, half the UK forces stated that fraud investigation was not specifically mentioned at all in force written policy, though it was sometimes covered in the course of more general policy statements on crime prevention and detection." (Levi .M, 2003: 41)

Levi goes on to describe how there is no uniformity in style, function and approach between the different police forces around the country. According to Levi, fraud squads suffer from being seconded to murder and major crime enquiries and the perception of fraud as being lengthy and complex.

This paper by Levi helps to put the relative importance of fraud investigations in the context of other efforts by the police. It can also be argued that the problems of detecting, preventing and prosecuting identity fraudsters are exacerbated by the apparent low priority fraud cases are given by the police. It was also estimated by the Credit Industry Fraud Avoidance System (2008) that the police investigate less than 1% of identity fraud cases. CIFAS notes that this due in part to the complexity of identity fraud

investigations and because that the investigations can often cross Police Authority boundaries and take up a great deal of time and resources.

Identity Crime – the Australian definition

The confusion over the contradictory nature of the terms identity fraud and identity theft is not only limited to America and Britain; in Australia concern over the issue of identity related crime has lead to a reorganising of the terms for official use. In Australia the concern over the differing uses of the terms identity theft and identity fraud lead to the adoption of another term identity crime. This term was adopted in policing circles and used to cover both identity theft and identity fraud. According to the Australasian Centre for Policing Research (A.C.P.R):

> "There does appear to be value in this approach. The classification helps distinguish identity takeover or assumption of a specific identity {i.e. identity theft} from a more remote and isolated use of an identity {or part thereof} for fraudulent purposes, usually involving financial gain or another form of benefit {i.e. identity fraud}. The above classification also helps to distinguish between the use of a fictitious identity and an existing or real identity. Such an approach should assist in the community's understanding of this phenomenon, as well as in marketing and community education initiatives." (Australian Centre for Policing Research 2004: 2)

The importance of establishing a clear definition of what constitutes identity crime is discussed in the SIRCA study by Cuganesan and Lacey (2003):

> "... prior research seldom discusses what is to be included as identity fraud and what is to be excluded. This lack of operationalisation results in significant ambiguity in interpretation." (Cuganesan, Lacey 2003: 23, cited in ACPR 2004: 3)

The ACPR report on standardising ID crime established definitions of the terms identity crime, identity fraud and identity theft in an effort to thoroughly cover the criminal activity made possible through the use of false identities. Proposed definitions used in Australia provided by Blindell (2006)

> "The term 'identity' encompass the identity of natural persons (living or deceased) and the identity of bodies corporate;
>
> 'Identity Fabrication' be used to describe the creation a fictitious identity;
>
> 'Identity Manipulation' be used to describe the alteration of one's own identity;
> 10
>
> 'Identity Theft' be used to describe the theft or assumption of a pre-existing identity (or significant part thereof), with or without consent, and, whether, in the case of an individual, the person is living or deceased;
>
> 'Identity Fraud' be used to describe the gaining of money, goods, services other benefits or the avoidance of obligations through the use of a fabricated identity; a manipulated identity; or a stolen/assumed identity;11 and
>
> 'Identity crime' be used as a generic term to describe activities/offences in which a perpetrator uses a fabricated identity; a manipulated identity; or a stolen/assumed identity to facilitate the commission of a crime(s).12" (Blindell .J, 2006: 1 of 1 see appendix 2 for original email)

Common themes in definitions of identity fraud and identity theft

By looking at the definitions used in these three countries, it can be argued that there are several key themes that are common to each. While each country has a different perspective on identity fraud and identity theft, it is clear that each country has encountered problems with distinguishing identity theft from identity fraud. The

Australian approach has been to invent a new term of identity crime in order to clarify the problem. But still in each country's definitions of the terms, the tendency has been to separate the two terms in order to apply them to different but similar identity related activities. Equally, each country's definition of identity fraud and identity theft highlights the trend to target individual identities and the form of dual victimisation this causes. It can be argued that it is as much the sense that an individual is losing control of their identity, as the actual crime committed that has caused the recent concern in identity fraud. Identity fraud and identity theft are new terms that refer to established forms of fraudulent criminal activity. The reason these terms have come into common use in the 21st century is due in part to statistical analysis which has shown an increase in the instances of identity related crime in the U.K.

An important organisation with regard to the statistical analysis of identity fraud is the Credit Industry Fraud Avoidance System (CIFAS). This system is responsible for compiling statistics on the levels of identity fraud in the U.K. CIFAS is a fraud prevention service with over 200 member organisations. These member organisations include representatives from banking, the credit card industry, telecommunications, asset finance, insurance companies and mail order companies. The system works through communication between these different groups and others on identified types of fraud in an effort to improve fraud prevention. According to CIFAS this system is the first of its kind in the world.

CIFAS argue that identity fraud is the fastest growing fraud type in the U.K. CIFAS records show that identity fraud has grown rapidly. In 1999, CIFAS recorded 9,000 cases of identity fraud; this number increased to 34,000 in 2002 and 80,000 in 2006. CIFAS also highlights the point that, while identity fraud may be a relatively rare crime, it is not a victimless crime:

"Identity theft is definitely not a victimless crime. In 2007, CIFAS identified and protected 65,000 victims of identity theft. As the scale and type of identity fraud varies, so does the impact on those whose identity has been stolen. In one-off cases, perhaps involving one fraudulent application or transaction, the damage to the victim may be minimal.

At the other extreme, persistent and skilled fraudsters who comprehensively steal an identity can cause a great deal of distress to victims. It can take between 3 and 48 hours of work for a typical victim to sort out their life and clear their name. In cases where a 'total hijack' has occurred, perhaps involving 20-30 different organisations, it may take the victim over 200 hours and cost up to £8000 before things are back to normal. They may suffer considerable (albeit temporary) damage to their credit status, which may then affect their ability to obtain finance or insurance - even a mortgage may be temporarily compromised." (CIFAS, 2007: 1)

Work done by CIFAS also looks at the fraudulent use of dead people's identities and notes that in 2003 there were 16,000 instances of this type of fraud. CIFAS note that in this type of fraud it is often very distressing for the family members to have the identity of their dead relative being abused. With respect to the cost of identity fraud CIFAS note that reported cases of fraud cost the U.K. economy £13.8 billion in 2002 and of this, identity fraud cost the U.K. economy £1.3 billion. CIFAS argue that this amount is conservative, as it does not include the costs incurred by local government and health services.

The statistics compiled by CIFAS on the rise in the instances of identity fraud, and the use of identity fraud by terrorists, illegal immigrants and organised criminals in recent years, have led to heightened media attention and the perception that identity fraud is *the* crime of the 21st century. This perception that identity fraud is a modern phenomenon is in part contradictory to the actual nature of identity fraud (see chapter 6 for history of identity fraud). When looking at the criminal activity covered by the terms identity theft

and identity fraud it is evident that it is the use of historically well established forms of fraud; that have evolved due to the use of new and developing technologies and cultural trends. The British Crime Survey for 2006/07 reported that an estimated 2% of the U.K. population had experienced the use of their personal details by someone else without their permission in the previous year. The identity fraud steering committee estimated the cost of identity fraud to the U.K. at £1.2 billion in 2006 -07(see appendix 1 for figures).

The overall cost of fraud to the U.K. was researched by Levi et al (2007) in *The Nature, Extent and Economic Impact of Fraud in the UK* they noted that fraud in general cost the U.K. approximately £13.9 billion in 2005. In reaching this number Levi et al note that there are difficulties in establishing an accurate number as to the cost of fraud given variations in definitions and the reporting of fraud.

> "...little is reliably known about the extent and cost of fraud in an aggregate sense. This considerably complicates policymaking. Much of what policy has had to be based upon is drawn from studies carried out by National Economic Research Associates (NERA) and Norwich Union to estimate the economic cost of fraud (NERA, 2000; Norwich Union, 2005). These place the cost of fraud in the UK at some 6.75 billion GBP as a lower bound and 13.82 billion GBP as an upper bound (NERA, 2000) and a (presumed mid-range) 15.78 billion GBP (Norwich Union, 2005). Neither study, however, represents the last word on the subject. Indeed, each makes clear that limitations in data quality and coverage make their figures tentative at best." (Levi .M, Burrows .J, Fleming .M.H, Hopkins .M, Matthews .K 2007: 5)

This problem over the accuracy of fraud figures is of particular importance in discussing identity related crime. In Levi et al's study it is noted that the term identity fraud is a problematic one as the scope of what constitutes identity fraud varies in the formulation of statistics by the organisations reviewed in Levi et al's study. In some respects it is argued that the use of the word 'identity' is redundant in discussion of

fraud as such a wide array of fraudulent activity is covered by the term. This point is elaborated on in Levi and Burrows (2008) paper *Measuring the impact of fraud in the U.K.* which discusses the findings of *The Nature, Extent and Economic Impact of Fraud in the UK*. In this paper they note that identity fraud is not a term which helps to assess the number of cases of fraud that occur.

> "...this study did not regard it as appropriate to treat ' identity fraud ' as a separate category of fraud, as some studies have done (Cabinet Office 2002; Home Office 2006) in response to popular concerns and a barrage of media interest. Like terrorism, it is a method of crime rather than a clear victim category, since it spans commercial businesses, financial institutions, governments and individuals." (Levi .M, Burrows .J, 2008: 304)

How fraud and fraud that involves some form of deception with regard to a person's identity is recorded is an important issue. It raises questions as to how accurate the perception that identity fraud is an emerging problem or indeed the extent of identity fraud in the U.K. The implication of separating and publicising identity theft and fraud over other forms of fraud is that it compels policy makers to address identity related crime as a new phenomenon. This further implies that new methods for combating identity related crime are needed such as the identity card scheme. However in practical terms determining as Levi et al's study implies the true level of identity related crime in society is not a simply task. The value of using terms such as identity theft and identity fraud in the formulation of statistics is also debatable.

Use of identity fraud by terrorists and organised crime groups

As well as looking at the theories surrounding the concept of identity fraud, it is also important to look at the different types of criminal who are associated with the use of identity fraud. The idea that identity theft and fraud is a major problem in the U.K. is in part based on the use of identity related crime by terrorists, illegal immigrants and organised crime groups. Arguably, what the identity card scheme seeks to prevent is not just the potential for someone to lie about who they are but also the systematic and

continued use of identity theft by organised groups. The September 11th 2001 terrorist attack in New York raised concern over terrorists' use of identity theft. The deaths of Chinese immigrants in 2004 at Morecambe Bay also raised concern over the levels of illegal immigrants in the U.K. This concern over the number of illegal immigrants entering the U.K has been linked to the use of false identification and organised crime in the form of people smugglers and human traffickers. Organised crime groups have also found identity theft to be a valuable source of income with some groups focusing and specialising in this activity.

Identity theft and fraud are activities that are hard to detect; they can enable clandestine travel and be a lucrative source of income. For these reasons, identity theft and fraud are an attractive option for terrorists, those involved in illegal immigration and organised financial fraud. The use of identity fraud by professional criminals such as conmen will be discussed in chapter 6. However, it is important to note that the argument for the introduction of a national identity card scheme has focused more on the threat posed by terrorists, organised crime groups and illegal immigrants than the activities of conmen. The following section will look at the use of identity theft and fraud by terrorists, those involved in illegal immigration and organised crime groups.

Terrorism and identity fraud

Since the terrorist attacks in New York September 11th 2001 there has been discussion with regard to identity fraud and its use by terrorists. The activities of terrorists are distinguished from those of a conventional armed force among other things by the fact that they conceal their presence within the general public. So the link between terrorism and the crime of identity fraud is in one respect is quite strong. In recent terrorist attacks by Islamic extremists there have been several incidents where terrorists have been discovered to be using stolen and false identities. Smith (2002) discusses the role and use of identity fraud by terrorist groups such as al Qaeda, and notes how the ability to travel undetected around the world is vital to their agenda:

> "Identity fraud and illegal migration have emerged as the lifeblood of global terrorism, as critical as any bomb, machine gun, or grenade. Terrorist organizations place a premium on clandestine international mobility, relying on an array of identity fraud techniques." (Smith .P, 2002: 7).

Gartenstien-Ross and Dabruzzi (2007) also note that the ability to avoid detection is of great value to those involved in terrorist attacks, and may involve fraud and deception:

> "The 9/11 Commission Report established that terrorists have committed identity fraud. 'For terrorists,' the Report noted, 'travel documents are as important as weapons. Terrorists must travel clandestinely to meet, train, plan, case targets and gain access to attack." (Gartenstien-Ross .D, Dabruzzi .K, 2007: 8)

According to Eldridge et al (2004) the first attack on the World Trade Centre in 1993 was enabled through the use of false identities and travel documents. Ramzi Yousef and Ahmad Ajaj who directed the attack, were caught in possession of numerous stolen identities, passports and drivers' licenses. After the 1993 World Trade Centre attack, but before Yousef was caught, he also used a false identity to board a Philippines Airline to plant a bomb which exploded but failed to crash the plane. Eldridge et al (2004) provide a case study of Yousef and Ajaj's activities to illustrate how the two used multiple false identities. (see appendix 3 for case study)

After the second attack on the World Trade Centre on September 11 2001, it was discovered that the same tactic of using false identities had been used. Every terrorist involved in the 2001 attack had used stolen social security numbers, and several used entirely false identities to succeed in their attacks. In a 2003 report by Tendler on the use of false identities by terrorists in the U.K. it is noted that:

> "The first two al-Qaeda terrorists convicted in Britain earlier this year were discovered with hundreds of false travel documents that had been used to open bank accounts, get a job and claim benefits." (Tendler .S, 2003: 1)

Aside from these accounts associated with the 9/11 attack, other members of al Qaeda have been discovered in possession of false identities. According to Raphaeli (2003), Dr Ayman al-Zawahiri believed to be Osama Bin Laden's second in command is one such member of al Qaeda known to have used false documentation. In December 1996 al-Zawahiri attempted to enter Chechnya in order to establish a base in the region but was caught by Russian security personnel. While ultimately the Russian authorities had to release al-Zawahiri due to a lack of evidence, during the trial and investigation it was found that al-Zawahiri had a variety of false documents in his possession. Raphaeli notes that among the documents found were visa applications, details for a Malaysian company which listed al-Zawahiri under an alias as the director, and various bank account details for both American and Chinese banks.

Identity theft and terrorist funding

Aside from helping in efforts to plan and commit terrorist attacks, identity theft is also noted by Gartenstien-Ross and Dabruzzi (2007) to be of value to terrorist groups in terms of funding their efforts. Since the end of the cold war, they argue, the need to rely on crime as a means of funding has increased as state sponsorship for terrorism has declined. They note that, in a broad sense, there are five areas of criminal enterprise where terrorist groups are known to have been involved: drug trafficking, financial fraud, illegal money transfers, illegal immigration and cyber crime. According to Gartenstien-Ross and Dabruzzi, of these areas financial fraud and identity theft in particular has been the most useful tool for raising funds. This point is echoed by Campana (2006), discussing identity theft in America. According to Campana:

> "...it should not be forgotten that most of all identity theft has a financial element. It is the sale and trading of stolen identities that links identity theft to drug trafficking, money laundering, organized crime, and terrorism." (Campana .J, 2006: 8).

Campana also highlights how the lack of awareness of identity theft in America is a problem for both individuals and organisations.

Border security and false documentation

Border security and the use of false documentation is another area in which identity fraud and terrorism can be connected. This subject has been discussed in some detail with regard to immigration control in America. Gartenstien-Ross and Dabruzzi (2007) note that violation of immigration control is often one of the first offences committed by terrorists. Kephart (2005) reviews the immigration history of 94 foreign terrorists. Of the 94 foreign-born terrorists who operated in the U.S between 1990 and 2004 Kephart notes that 59 committed immigration fraud prior to or conjunction with taking part in terrorist activity. Of these 59, many conducted multiple immigration violations - 79 in total according to Kephart. The main concern in the report is the apparent ease with which terrorists were able to enter the U.S and stay in the country and maintain the appearance of legitimacy:

> "What requires emphasis is the ease with which terrorists have moved through U.S. border security and obtained significant immigration benefits such as naturalisation. The security gaps that existed then still, in many instances, exist today. My work on the 9/11 Commission made it clear that terrorists need travel documents for movement at some point during their journey here as much as they need weapons for operations. Once within U.S. Borders, terrorists seek to stay. Doing so with the appearance of legality helps ensure long-term operational stability. At the 9/11 Commission we called this practice *embedding*, a term also used in this report" (Kephart .J, 2005: 7)

The issue of border control and the use of false documentation is also of importance with regard to the issue of illegal immigration and people smuggling and is discussed in that context later in this chapter.

Organised crime and the use of identity fraud

In many of the modern cases of identity fraud discussed in this thesis, understandably, the main motivation to commit fraud has been financial. Aside from being a difficult crime to detect, identity fraud can also be a lucrative criminal enterprise, espccially if it involves multiple victims. A noteworthy example of organised crime using identity fraud is the use of advanced fee fraud by Nigeria based organised crime syndicates, known as the Nigerian 419 scam. The Nigerian 419 scam involves convincing victims to provide a sum of money on the promise that eventually it will lead to them being given a greater sum. The process underlying Nigerian 419 scams and advanced fee fraud are presented in chapter 6. In this section, the focus will be on the groups who use Nigerian 419 scams. An important source of information on the people who engage in this activity is a Watchdog group known as the 419 Coalition. On the Coalitions main webpage it is noted that:

> "The Nigerian Scam is, according to published reports, the third to fifth largest industry in Nigeria. It is the 419 Coalition view that the elites from which the governing classes of Nigeria are drawn contain 419 Scammers which can make it difficult for victims seeking recourse in these matters. Monies stolen by 419 operations are very rarely recovered from Nigeria, although the Nigerian Economic and Financial Crimes Commission (EFCC) led by Nuhu Ribadu and Ibrahim Lamorde made some welcome progress in that regard over the last few years." (419 Coalition, 2009: 1-2)

According to the 419 Coalition the 419 scam is operated predominantly from Nigeria but also from other West African nations such as Ghana, Togo, Liberia, Sierra Leone and the Ivory Coast. The coalition estimate that the scam began in the 1980s and by 1996 had made the gangs who run the scam $5 billion; they also believe that this sum has gone up since 1996.

The emergence and success of 419 scams is discussed in Wright (2006). Wright refers to the work of Ebbe (1999) who argues that a symbiotic relationship has developed between the government and criminals. Wright (2006) describes how:

> "Organised crime and the legitimate economy of the country are closely integrated. Nigerian criminal gangs operate from a territory that is notorious for its corruption." (Wright .A, 2006: 157)

The combination of corruption in Nigeria and the increase in globalisation is the key to the success of the 419 scam. Initial the scam in the 1980s involved the use of fax machines to convey the scam message to victims. Eventually criminals involved in the scam transferred to the use of the internet and emails. According to Finckenauer and Albanese (2005) aside from Nigerian and West African organised crime groups, Russian organised crime groups based in America have also used and relied on fraud as a criminal enterprise.

Efforts to police identity related crime

According to the National Criminal Intelligence Service and its successor the Serious and Organised Crime Agency (SOCA), crimes such as organised immigration crime, money laundering and fraud against individuals and the state are enabled through the use of false and/or stolen identities. An assessment by the National Criminal Intelligence Service concluded that while it was difficult to make firm judgements on the extent to which identity fraud is used by organised crime it could be determined to a reasonable degree that:

> "a. Identity fraud underpins much serious and organised crime. A significant proportion of criminals at all levels use false personal identities;
> b. Identity fraud cuts across most criminal sectors: illegal immigration, drugs trafficking, money laundering, vehicle theft, and fraud against the public sector;
> c. The primary purpose of false identities is to enable serious and organised criminals to conceal themselves, their activities and their assets. They may also

facilitate specific criminal's acts, such as people smuggling or benefit fraud. In addition, false identities are sold for money;

d. A false identity document can be obtained by counterfeiting or forgery, fraudulent application or misuse of someone else's document. Theft and corruption can play a supporting role. Some serious and organised criminals undertake these activities themselves; others turn to their contacts or to specialist providers to meet their needs;" (National Criminal Intelligence Service, 2003: 2)

The assessment also determined that counterfeiting and forgery were the most common methods used by organised and serious criminals as a means of obtaining false identities. In April 2006, the Serious and Organised Crime Agency was formed as part of the Serious and Organised Crime and Police Act 2005. This agency took over from the National Crime Squad and National Criminal Intelligence Service; the agency also took over the investigative and intelligence gathering work of Her Majesty's Customs and Excise with regard to drug trafficking and the Immigration Services work on organised immigration crime. This agency also highlights the role of identity fraud in the activities of organised crime, noting its use in private and public sector fraud. According to the 2007/08 Annual Report by SOCA, the agency has conducted operations which focus on efforts to combat illegal immigration and identity fraud. Operations which are noteworthy are operation Coptine which investigated people smuggling and the use of false documentation, and Operation Ajowan which targeted the trade in credit information.

Operation Coptine was a five year operation which looked into an organised crime group who were smuggling Indian illegal immigrants from South Africa to the U.K. The group, based in Leicester, would smuggle Indian nationals to South Africa and then through the use of fake or stolen passports would enable these illegal immigrants to come to the U.K. The gang also engaged in credit card fraud and visa scams. The report estimated that the criminals involved had made £5 millions and Operation Coptine resulted in the arrest of 200 people worldwide with 40 members of the group being prosecuted in the U.K. According to O'Neil (2008) the gang smuggled an estimated

6,000 illegal immigrants into the U.K. and charged between £5,000 and £8,000 per migrant. The gang was lead by Yusef Mewaswala who was convicted and sentenced to ten years in prison.

Another operation conducted by SOCA which involved identity fraud was Operation Ajowan which investigated the trade in stolen bank and credit information via the internet. According to the 2007/08 report by SOCA:

> "The potential loss to the UK from the actions of just one of the conspirators was assessed at over £6m." (SOCA, 2007/08: 28).

Aside from SOCA, identity fraud is also investigated by the Economic and Specialist Crime Unit which is responsible for investigating a variety of different forms of fraudulent activity. Within the Economic and Specialist Crime Unit there are several operations focused on preventing and detecting criminal activity which involves the use of false or stolen identities. Operations Maxim and Sterling are directly involved in combating identity fraud and the use of false identities. Operation Sterling is the name given to the Metropolitan Police Services strategy to commit economic crime in London. This operation has involved forming partnerships between the Metropolitan police and several public and private industries. Through Operation Sterling, the Metropolitan Police are trying to identify where organised criminals are using identity fraud and how to prevent it. Operation Maxim is dedicated to investigating cases of people smuggling and human trafficking. Within this operation is Project Genesis a joint operation between the police and the printing industry to prevent the abuse of printing equipment. On 21st March 2007 an investigation lead by Operation Maxim resulted in 13 raids across London on illegal passport factories and suppliers. These raids resulted in 22 people being arrested, with £40,000 being confiscated along with a variety of fake passports, drivers' licences and foreign identity documents.

While the Economic and Specialist Crime Unit is involved in combating identity fraud, the overall involvement of the police in investigating identity fraud has been criticised by some. According to the Credit Industry Fraud Avoidance System (CIFAS) less than one per cent of identity fraud cases are investigated by the police. CIFAS notes that many cases of identity fraud are time consuming and cross several police authority boundaries, making the policing of this type of crime problematic.

Organised crime and illegal immigration

One area of criminal activity where the use of identity fraud by organised crime groups can be seen most clearly is in the use of identity fraud to facilitate illegal immigration. As with concern over identity fraud and its use by terrorists, the use of identity fraud by illegal immigrants and organised crime groups gained increased public awareness at the beginning of the 21st century.

In 2000 concern over illegal immigration was raised with the discovery of 58 dead illegal immigrants in a cargo container in Dover (Kyle, Liang, 2001: 18). All were from the Fujian province of China and had died from suffocation. This incident was followed in 2004 with the reported deaths of 23 Chinese illegal immigrants working as cockle pickers at Morecombe Bay.

When discussing illegal immigration, important issues to consider are the role and activities of people smugglers, the use of false documents such as passports and the degree of involvement of illegal immigrants are with criminal activity after entering the U.K. The use of false documentation and the role of people smugglers are discussed in the House of Commons Home Affairs Committee Second Report on Asylum Applications (2003-2004). According to the report, a large proportion of asylum seekers who enter the U.K. do so through people smuggling operations. It is noted in the report that asylum seekers use illegal methods of entry into the U.K. because of visa restrictions and the difficulty of gaining entry. In the report, Beverley Hughes MP, Minister of State at the Home Office, states :

> "I would say the vast majority, either through actually being transported in lorries and so on through people operating as people smugglers, or through facilitation at the other end or with false documents that allow people to get on an airline." (House of Commons Home Affairs Committee, 2003-04: 30)

Input into the report is provided by Harriet Sergeant, author of the Centre for Policy Study's pamphlet *Welcome to the Asylum*(2001). In the report, Sergeant discusses the role in illegal immigration of people smugglers and false documentation:

> "This new migration industry provides all kind of services to would-be immigrants from obtaining entry visas and other supporting documents for travel, to transport arrangements and legal instructions on how to apply for asylum and employment. A journey from Asia, India and Pakistan, costs about £15,000 to £20,000. A Franco-Dutch gang active since 1994 charges Chinese immigrants $50,000 for their journey to the US which includes new identities and false passports. A large market has grown up for forged documents." (Sergeant.H cited in House of Commons Home Affairs Committee, 2003-04: 30)

The trade in false passports and documents was investigated in a 2006 Panorama documentary *'My fake passport and me'*; journalist Shahida Talaganova illustrated how people are able to obtain false or stolen passports all over the European Union and former Soviet countries. Talaganova then showed how these documents are used to enter the U.K. illegally. The goal Talaganova set herself in this documentary was to obtain a fake passport from each of the 24 member states of the E.U. Then Talaganova planned to enter the U.K. illegally by using these passports. Throughout the documentary Talaganova travelled to various countries in the E.U. and former Soviet Union countries such as the Ukraine. In each country Talaganova sought out brokers who deal in stolen and fake passports. In many instances, the brokers stated that rather than providing a stolen passport they would find someone from an E.U. country to apply for a passport and then substitute the picture for a picture of Talaganova.

When Talaganova successfully obtained a number of passports this way she took them to an expert in forgery who checked each one under a ultraviolet light to detect the hidden security layers in the laminate used in passports. After choosing the best fake passport Talaganova then attempted to enter the U.K. Talaganova took a ferry from Spain to the U.K., and despite being checked by immigration officials, was able to enter the country on a Latvian passport.

Aside from obtaining falsely applied for passports, Talaganova also attempted to obtain a stolen passport and then have it altered. The documentary shows how the influx of holiday makers in Barcelona, Spain, during the summer is a good time for illegal immigrants to obtain a stolen passport. In Spain, Talaganova was able to obtain stolen passports from Holland, Portugal, Belgium and the U.K. By the end of her investigation, Talaganova had been able to obtain passports from 20 of the 24 member states of the E.U. Her investigation only stopped after a dangerous encounter with one broker in false passports who threatened her with a knife. The documentary ends with Talaganova gaining entry to the U.K. using the stolen Dutch passport obtained in Spain. Talaganova entered the U.K. on the Eurostar train and successfully passed two security checks in Belgium and the U.K.

What this documentary highlights is the well developed market in fake or stolen passports that exists in both the E.U. and those countries which border the E.U. It also highlights the differing attitudes held towards illegal immigration. In one instance in Greece, Talaganova was told how the police will accept the presence of illegal immigrants as they are aware that they do not want to stay in Greece but rather they are travelling to the U.K. and if they arrest them they will only be ensuring that they stay longer in Greece. Furthermore people smuggling provides organised crime with a source of income comparable to drug and arms smuggling.

The issues raised with regard to false documentation in Talaganova's documentary are also discussed in a Europol (2008) report on illegal immigration: *Facilitated Illegal Immigration into the European Union.* In this report, Europol also note that false

documents are used to enter the European Union and that these documents are often produced by organised crime groups. Moreover:

> "Although travel documents, such as passports, national ID cards, visas and residence and work permits, are the most commonly falsified travel documents, a number of other types of documents are targeted by OC groups. Documents needed to support bogus application for a business or student visa are frequently falsified. These kinds of documents may include registrations for a school or a study, supporting letters from an employer or an invitation from a company within the EU. The use of other documentation, such as seaman books and joining letters from shipping companies and the merchant navy are also used to allow illegal immigrants to enter or transit the EU without visa." (Europol, 2008: 4)

Living as an illegal immigrant

Aside from enabling illegal immigrants to enter the U.K., people smugglers and false documents also have a part to play in enabling illegal immigrants to stay in the country. Housing, work and health care are all aspects of living in the U.K. that illegal immigrants are able to access. Through people smugglers and false documentation, access to these things can be made easier. The level of interaction between smugglers and illegal immigrants varies, as does the care and attention the smugglers give to illegal immigrants.

A distinction can be made between those organised crime groups which smuggle people and those who traffic in human beings. According to Nicola (2004) the activities of people traffickers can be broken down into three stages: recruitment, transfer and entrance into the destination country. Human traffickers by contrast engage in another stage after transportation to the destination country and this further stage is exploitation. In both people smuggling and human trafficking, false documentation can play a vital role in transporting of migrants and maintaining

control over them. The relationship between people smugglers and illegal immigrants is discussed by Enzensberger (1992) who says

> "Illegal migration and illegal employment presupposes illegally operating entrepreneurs. Organised crime provides a service to such entrepreneurs, as they smuggle human beings on request. 'In the textile industry the unskilled sector and, above all, the building trade, practices dominate which are reminiscent of the slave markets of the past." (Enzensberger, 1992 cited in Ruggiero .V, 1996: 140)

This viewpoint suggests that, in the relationship between illegal immigrants and people smugglers, the power resides with the people smugglers who are in control of both the illegal immigrants' travel into the country, and their residence and employment. However according to Margaret Beare in Phil Williams (1999) book *Illegal Immigration and Commercial Sex: The New Slave Trade:*

> "As one smuggler said: 'First of all, I never go out to look for clients. Invariably it is the client who comes to me for help.... Second, I do not traffic in drugs or ammunition. My work hurts nobody. In fact, it helps people'." (Beare .M.E, in Williams .P, 1999: 23-24)

The discussion of illegal immigration can at times focus on the oppression and subjugation of illegal immigrants by organised crime groups. Equally it is important to remember that for those who become illegal immigrants the perceived benefits outweigh the risks. Chawla and Pietschmann (2005) in their chapter on *Trafficking in Human Beings and Smuggling of Migrants* in the *Handbook of Transnational Crime and Justice* discuss how globally there is still a gross disparity in terms of income between the rich and poor. They refer to findings from the U.N. Development Programme 2002 which note the following:

- In 1999, 2.8 billion people lived on less than $2 a day, with 1.2 billion of them barely surviving at the margins of subsistence on less than $1 a day.
- The richest 5% of the world's people have incomes 114 times those of the poorest 5%.
- During the 1990s the number of people in extreme poverty in Sub-Saharan Africa rose from 242 million to 300 million (U.N Development Programme, 2002: 10)

These issues and others are raised by the U.N. Development Programme to illustrate the current state of human development. It is also noted that there has been a drop in the proportion of people around the world living in extreme poverty from 29% in 1990 to 23% in 1999. However in Chawla and Pietschmann's (2005) chapter the negative aspects of human development are focused on and discussed in terms of their influence on the decision of people to become illegal immigrants. They argue that people smugglers and traffickers in human beings exploit the needs of the impoverished who are seeking a better life:

> "The difference of well being among the countries of the world, and perceptions of those differences, are the main factors not only for emigration but also for the criminal activities of migrant smuggling and trafficking in human beings." (Chawla .S, Pietschmann .T, 2005: 184)

Chwala and Pietschmann also refer to push and pull factors which influence people's decision to become a migrant. Push factors motivate people to leave the country they live in, and pull factors attract migrants to a particular country or region. Europol in a report on the *Trafficking in Human Beings in the European Union: A EUROPOL Perspective* (2008) outline the different push and pull factors:

Push Factors

- high unemployment
- labour market not open to women and gender discrimination
- lack of opportunity to improve quality of life
- sexual or ethnic discrimination
- poverty
- escaping persecution, violence or abuse
- escaping human rights violations
- collapse of social infrastructure
- other environmental conditions including conflict and war

Pull Factors

- improved standard and quality of life
- better access to higher education
- less discrimination or abuse
- enforcement of minimum standards and individual rights
- better employment opportunities
- demand for cheap labour
- demand for commercial sexual services
- higher salaries and better working conditions
- demand for workers within the sex industry and higher earnings
- established migrant communities (Europol, 2008: 3)

According to Europol, all EU countries are affected by illegal immigration but, there are certain countries which are the main destinations for illegal immigrants and victims of human trafficking. These countries are Austria, France, Germany and the United Kingdom. These countries are the most desired destinations for migrants and organised crime groups exploit this desire by promising employment opportunities. Europol note that there is no typical victim of human trafficking. According to the Office for Victims of Crime:

"Each year, an estimated 600,000 to 800,000 men, women, and children are trafficked across international borders (some international and non-governmental organizations place the number far higher), and the trade is growing. (U.S. Department of State. 2004. *Trafficking in Persons Report*. Washington, D.C.: U.S. Department of State.)

> Of the 600,000-800,000 people trafficked across international borders each year, 70 percent are female and 50 percent are children. The majority of these victims are forced into the commercial sex trade." (Office for Victims of Crime, 2005: 1)

The key to human trafficking is the exploitation of the desire of migrants to gain a better life and this is done this through false promises of work and control over their movement, documentation and contact with others.

Human trafficking and false documentation

False documentation and the control of migrants' documentation can be an important factor in the trafficking of women for sexual exploitation. There are different types of human trafficking operations; some operations traffic in people in order to exploit them for labour in the hidden economies of countries (see below for discussion of hidden economy). Others are sex trafficker operations which seek to exploit women and children. According to Hughes (2000) in her paper - *The "Natasha" Trade: The Transnational Shadow Market of Trafficking in Women,* one method of recruiting and controlling women used by sex traffickers is to utilise false documentation:

> "Some traffickers use the woman's legal documents and tourist visas to legally enter the destination countries. The woman may be put on a circuit by pimps in which they are moved from country to country on legal tourist visas or entertainers visas. Other times, the woman is given false documents. In this case, the woman is even more vulnerable after she arrives in the destination country because she is there illegally. If police discover her she is arrested and deported." (Hughes .D, 2000: 6)

According to Caldwell et al. (1999), false passports are also used to conceal the age of young girls being smuggled by gangs:

> "...'Natasha', a Moscow-based Russian citizen who traffics woman and girls to Japan to work as prostitutes, informed GSN that she could obtain foreign passports for underage girls. 'According to our rules' she said, 'you must obtain an international passport. But, to go abroad, if she is only 16, she must get approval from her parents. If you want to avoid it, we can make her a passport where it will be indicated that she is 18, so she doesn't need to have any approvals. " (Caldwell .G, et al, 1999: 48)

This discussion of illegal immigration focuses on the activities of people traffickers who exploit the illegal immigrants they smuggle. However, not all operations end with the exploitation of migrants; there are some migrants who try to integrate with legal citizens.

Illegal immigrants and 'looking legitimate'

A study conducted by Engbersen and Van Der Leun (2001), – *The Social Construction of Illegality and Criminality,* conducted research into the relationship between migration and criminality, looking at the degree to which illegal immigrants engaged in further criminal activity. This study involved interviews with 170 illegal immigrants living in Rotterdam in Holland between 1993 and 1998. Engbersen and Van Der Leun found that:

> "Apart from the use of false or forged documents which the respondents considered unavoidable, the majority of the interviewed illegal immigrants refrain from criminal activities, They do everything they can to keep on the right side of the law and commonly find other ways of making a living." (Engbersen .G, Van Der Leun .J, 2001: 56)

Engbersen and Van Der Leun also note that figures on the arrest of illegal immigrants showed that 47% of illegal immigrants were arrested for illegal residence which was the most common reason for arrest. The study by Engbersen and Van Der Leun is useful when looking at illegal immigration in the U.K. It suggests that while illegal immigrants might rely on false documentation and people smugglers to enter a country, there is no guarantee they will continue to engage in criminal behaviour. It can be argued that continued involvement with illegal activity would jeopardize migrants' efforts to remain in the country by increasing the chances they will come into contact with the police.

However involved the illegal immigrants are with the people who smuggled them into the country, they will have to gain some form of employment. In a report by Lord Grabner on the Informal Economy (2000), the issue of employing illegal immigrants is discussed.

Hidden/informal economy

According to Lord Grabner the informal economy (sometimes referred to as the hidden economy) refers to undeclared economic activity where no income tax, National Insurance contributions or Value Added Tax (VAT) are collected or claimed. The informal economy covers a number of different activities, such as tax evasion, working while claiming some form of unemployment benefit and running an unregistered business. With regard to illegal immigrants working in the United Kingdom Lord Grabner states:

> "Broadly speaking, illegal immigrants are prohibited by law from working. It is also illegal for employers to hire them. Employers have a duty to check that new employees have a right to work. So, by definition, if illegal immigrants do work, they are part of the informal economy." (Lord Grabner, 2000: 16)

Lord Grabner goes on to explain that assessing the number of illegal immigrants in the U.K. is difficult, but that the majority of illegal immigrants have been found to work in sectors where the work is casual and paid with cash in hand. Lord Grabner also notes that some employers deliberately hire illegal immigrants as they are a source of cheap labour. The use of illegal immigrants also means that employers can avoid implementing health and safety regulations, and can avoid paying the national minimum wage as their employees are unlikely to complain for fear of exposing themselves to the authorities.

With regard to identity fraud, Lord Grabner discusses the subject in the context of defrauding the benefit system and the illegal use of National Insurance numbers. National Insurance numbers are unique numbers that are issued to people in the United Kingdom when they reach 16, and are used when applying for benefits or starting work as an employee. National Insurance numbers are sometimes issued to adults from abroad who come to live in the U.K. and it is here that instances of fraud have been found. National Insurance numbers can be used fraudulently if someone who is not entitled to work in the U.K. can obtain one. Lord Grabner also discusses the use of birth certificates of dead people by fraudsters to make multiple claims for state benefits. The importance of investigating the informal economy is that it is one of the reasons people enter this country illegally and why people are able and ready to create and use false identities.

It has been difficult to find statistics on the number of illegal immigrants in the U.K. and in 2006 the National Statistics review by the Home Office acknowledged this by calling for a more in-depth study of the number of illegal immigrants in the U.K. Current estimates from the Home Office estimate that there are between 310,000 and 570,000 illegal immigrants in the U.K. Of this population, it can be speculated, a percentage are involved in the use of identity fraud.

Identity cards as a means of preventing organised crime, illegal immigration and terrorism

Identity related offences are vital parts of many criminal enterprises; terrorists, illegal immigrants and organised crime groups all benefit in some way from using identity theft. In the debate over the introduction of the identity card scheme much has been made of the idea that identity cards can prevent the use of identity related crime by these groups of offenders. According to Lyon (2004):

> "At least three kinds of arguments are used to promote ID systems; eliminating terrorism, preventing fraud and controlling immigration. The first works on the logic of security and fear, the second on that of management and audits and the third on legal residence—who may be in the country and what they may do while there. ID cards, it seems, can provide simultaneous solutions to several perceived problems." (Lyon .D, 2004: 4)

The U.K. identity card scheme has been promoted by the government on the basis of these three arguments. The emphasis has for the most part been on preventing the activities of terrorists, illegal immigrants and/or organised criminals rather than using the identity card to specifically target these types of criminals. It has been argued by the government that, by denying access to identity related crime, the scheme can deter and/or detect any and all individuals involved in criminal activity. When the Entitlement Card Scheme was first unveiled in 2002, a great deal was made of the crime prevention benefits:

> "Biometric ID cards will provide a simple and secure means of verifying identity. Together with electronic border controls they will help us tackle illegal migration and working, organised crime, terrorist activity, identity theft, and fraudulent access to public services, as well as helping our citizens travel freely and complete everyday transactions securely and easily. (Blunkett.D cited in Privacy International, 2004: 1)

This argument that the identity card scheme can help in preventing crime has remained central, despite criticism from opposition parties and protest groups. In a 2008 speech by then Home Secretary Jacqui Smith, the idea that the identity card scheme could prevent crime was still a vital part of the argument for introducing the scheme:

> "...the duty of public protection and the impetus for greater citizen convenience are the two drivers for our plans for the National Identity Scheme.
>
> The benefits are clear:
>
> • to counter illegal immigration and illegal employment;
>
> • to tackle crime and terrorism;
>
> • to lessen the burden for employers and employees involved in proving identity;
>
> • to improve access to the public services to which we are entitled; and
>
> • to, quite simply, make life easier for all of us in the modern world." (Smith .J, 2008: 9)

The identity card is presented as a multi purpose solution to the problem of identity related crime by preventing people from using multiple identities. With a secure means of identification in operation terrorists cannot embed themselves in the civilian population. Illegal immigrants cannot pass themselves off as legitimate residents and organised criminals cannot capitalise through financial fraud, people smuggling or human trafficking. It is envisaged that individuals contemplating identity related crime in the U.K. will be deterred from even trying.

According to former Home Secretary Jacqui Smith, the identity card scheme will prevent the creation of multiple identities by terrorists and organised criminals. Smith argues that the identity card will combat terrorism and organised crime by preventing money laundering which can involve the use of false identities to establish bank accounts. Smith further argues that the introduction of the National Identity Card Scheme has helped prevent identity related crime by introducing legislation that criminalises the use of false identities.

On the issue of terrorism there has been a significant amount of criticism over the idea that identity card can prevent terrorist attacks. An important part of the argument for the introduction of the identity card scheme has been the preventing terrorist from using multiple identities in the U.K. As discussed earlier, the success of the September 11th attacks was in part due to the terrorist's ability to embed themselves within the civilian population. However, both the July 7th 2005 attacks on London and the 2007 attack on Glasgow were conducted without the need for any identity related crime. The terrorists involved were U.K. citizens who would have been eligible for an identity card had the scheme been in effect. Critics such as Mendham (2004) argue that the government is playing on the general public's fear of terrorism in order to introduce the identity card scheme:

> "Following the 11th September atrocity, the UK Government immediately began talking about introducing ID Cards. We were told they would help fight crime and specifically terrorism. In fact this was simply a case of Blunkett shamelessly taking advantage of the post-911 panic. There is no evidence to support the claim that ID Cards will significantly cut down on crime and terror. Many other countries have ID Cards and still suffer from crime and terrorism." (Mendham .T, 2004: 1)

The role of the identity card scheme in preventing terrorist use of identity theft and fraud is discussed in more detail in chapter 9. The arguments raised with regard to the effect identity cards might have on terrorist activities are also important when discussing the actions of organised crime and illegal immigrants. As stated earlier, identity related crime is important to both terrorists and organised crime because it enables clandestine travel and a means of criminal enterprise. According to the U.K. Border Agency, the identity card will help with the detection of illegal immigrants by confirming the status of immigrants to the U.K.:

> "It is a very secure way to provide evidence of the holder's nationality, identity and status in the United Kingdom. It helps public agencies, employers and educational establishments to more easily understand the migrant's entitlements.

> It also enables holders to confirm their identity, immigration status, and right to work or study and access public services." (UK Border Agency, 2009: 1)

The ability to confirm people's migration status and their eligibility is, according to the government, key to preventing illegal immigration. By obtaining biometric records of foreign nationals in the U.K., the scheme will be able to separate legal residents from illegal immigrants. With regard to immigration, the identity card scheme would also allow the government to keep track of failed asylum applications in order to catch anyone trying to stay in the country. However, Mendham argues that with regard to illegal immigration the identity card scheme could conceivably cause a rise in crime:

> "ID cards will not deter illegal immigrants, they will still come. Nor will ID Cards allow illegal immigrants to be deported more easily. By definition people in the country illegally will not apply for the cards and will avoid places where these cards need to be shown. Most illegal immigrants currently work at the fringes of legality, where pay is in cash, no questions asked. Such employers are unlikely to start demanding to see Identity Cards. If they do then many illegal immigrants will have no choice but to turn to crime to survive. Thus compulsory National Identity Cards could actually raise the crime rate." (Mendham .T, 2004: 1)

By introducing the National Identity Card scheme, the government seeks to provide a multi purpose solution to the activities of several groups of offenders. How will criminals react to the identity card scheme? The desired effect is that the scheme scares anyone considering identity theft by presenting a system which guarantees detection of any identity related crime. However it can be argued that rather than being scared by the identity card scheme, criminals will adapt their behaviour to compensate for its presence. It is foreseeable that terrorists and organised criminals may attempt to compromise the scheme through the use of corrupt employees or advances in forgery. It may be that terrorists and organised criminals simply adapt their activities to avoid interaction with the identity card scheme.

Law regarding fraud

Identity theft and identity fraud have yet to be codified as crimes but there are numerous criminal offences under current legislation which can be considered forms of identity theft and identity fraud. Just as determining the extent and nature of the term identity can be a complicated matter, examining how the law responds to identity fraud is also a difficult issue.

Identity fraud is an abuse of the identification process but this does not always mean it is an abuse of the law. This could be because the actual abuse of the identification process does not contravene any legal statues or there is no expectation of ownership over the information or identification.

For instance obtaining another person's birth certificate is not a crime, they can be purchased by anyone (e.g. people interested in genealogy). Equally, obtaining someone's birth certificate is not a crime against that person as they have no right to sole ownership of that form of identification. The issue of privacy is also a key factor in the determination of the legality of identity fraud and changing identity.

The criminality of modern identity theft and identity fraud is a dual criminality, firstly against the individual whose identity is stolen, and secondly against the third party who has entered into some form of interaction with the person using another person's identity. The development of the concept of a crime of deception as outlined in the 1968 and 1978 Theft Act form the basis for crimes that can be defined as identity fraud. More recently the 2006 Fraud Act also helps to outline what crimes can be considered identity fraud.

1968 and 1978 Theft Acts – crimes of deception

When determining the criminality of identity fraud in the U.K. the first area to look at is the crime of deception as it is described in the 1968 and 1978 Theft Acts. Under section 15{4} of the 1968 Theft Act, the concept of deception is defined as –

> "For the purpose of this section 'deception' means any deception {whether deliberate or reckless} by words or conduct as to fact or as to law, including a deception as to the present intentions of the person using the deception or any other person" (Section 15{4} 1968 Theft Act cited in Herring .J, 2006: 570)

Under the 1968 act, the key elements to deception were that by word and action an individual had deceived on the grounds of fact or law. When establishing if a criminal deception has taken place under the 1968 act, a person's statements must be determined as untrue and someone must be victimised by the deception. The requirement that a person is victimised in order for there to be a crime of deception means that crimes which involve counterfeit objects and machines (e.g. fake debit cards in ATM machines) are crimes not of deception but rather of theft.

When discussing crimes of deception the following terms are important: obtain, procure, secure and induce. In order for a theft to be considered a crime of deception the criminal must obtain, procure, secure or induce some result through deception. The 1968 act outlines several different types of criminal deception. Arguably there are many forms of identity fraud which would be prosecuted under sections of the 1968 Act. Below are several examples of sections from the 1968 and 1978 Act.

1. Obtaining property: 1968, s.15.
2. Obtaining a pecuniary advantage: 1968, s.16.
3. Procuring the execution of a valuable security: 1968, s. 20{2}.
4. Obtaining services: 1978, s. 1.
5. Securing the remission of a liability: 1978, s. 2{1} {a}.
6. Inducing a creditor to wait for or to forgo payment: 1978, s. 2{1} {b}.
7. Obtaining an exemption from or abatement of liability: 1978, s. 2{1} {c}.

(Smith J.C, 1989: 84)

2006 Fraud Act

The most recent improvement to U.K. law with regard to fraud is the 2006 Fraud Act. This act focuses on three areas of fraud and more directly deals with the types of criminal behaviour referred to as identity fraud. The 2006 Fraud Act addresses the crimes of fraud by false representation, fraud by failing to disclose information and fraud by abuse of position. All three types of fraud discussed in the 2006 act can be considered forms of identity fraud.

Under section 2 of the act a person has committed fraud by false representation if they have dishonestly made a false representation and if by making this false representation, the individual intends to gain from this deception for themselves or another. Also, under this section, if an individual intends to use false representation to harm another by causing them to lose something or put them at risk of loss then they have committed a crime.

This section covers activities such as applying for credit in someone else's name or using another person's credit details to draw money from their account. Section 2 goes on to explain what exactly is meant by a false representation. According to the act:

> "{2} A representation is false if-
> {a} it is untrue or misleading, and
> {b} the person making it knows that it is, or might be, untrue or misleading
> {3} 'Representation' means any representation as to fact or law, including a representation as to state of mind of-
> {a} the person making the representation, or
> {b} any other person.
> {4} A representation may be express or implied
> {5} For the purposes of this section a representation may be regarded as made if it {or anything implying it} is submitted in any form to any system or device designed to receive, convey or respond to communications {with or without human intervention}." (Fraud Act 2006, c 35: 2)

The 2006 act abolishes several sections of the 1968 and 1978 theft act with regard to crimes of deception. Through the 2006 act the criminal activity of those involved in identity fraud has been addressed. The criminalising of false representations does however raise some questions as to the extent of this law and whether or not it allows for any personal freedom with regard to presentation of self. As the act focuses on the issue of representation it is necessary to ask what false representations are not criminal? If a person alters their first name or uses their middle name are they liable under the new law?

American law on identity theft

America's response to the crime of identity theft has been to introduce new laws specifically designed to prosecute people involved in identity theft. This law is the Identity Theft and Assumption Deterrence Act 1998 which outlines the crime of identity theft and provides some parameters for prosecutors to determine what identity theft is and if someone has committed it.

> "(7) knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law;." (Identity Theft and Assumption Deterrence Act, 1998: Section 1028(a) of title 18)

Other laws on identity theft in America include the Gramm-Leach-Bliley Act 1999 which outlaws the use of pretexting (also known as social engineering, see chapter 7). The act requires that financial institutions take all precautions necessary to protect and defend the consumer and associated non-public information from identity thieves who use pretexting to obtain information. However, according to Sullivan (2004) there are rules in place to outlaw this method of appropriating information and thereby committing identity theft. Private companies and financial institutions have been slow to adhere to the requirements laid out in the Gramm-Leach-Bliley.

The fact that America has laws against identity theft does not mean that identity theft is a high priority for prosecutors or the police in America. Sullivan goes on to argue that for police and prosecutors there is very little motivation to prosecute identity theft as the crime often requires a great deal of investigation and prosecution is at times difficult.

Conclusion

In conclusion, identity fraud is form of criminal activity which has recently received attention both in the U.K. and abroad. In all definitions, however there are common themes, such as the emphasis on distinguishing and using both the terms identity fraud and identity theft. Also criminological study of identity fraud has looked primarily at the abuse of an individual's *personal identity* and acts of deception with regard to an individual's personal identity. This emphasis on the abuse of personal identities is due in part to a perceived rise in the abuse of personal identities as noted by recent surveys of identity fraud. Also accounts of the experiences of victims of identity theft help to emphasise the personal and financial harm caused by this non-violent, white collar crime. The apparent rise in popularity of identity fraud by organised crime groups, illegal immigrants and terrorists has also helped to make identity fraud an important issue in the 21st century. The idea that there are people in society being deceptive about their 'true' or 'legitimate' identity has raised the general level of concern over the safety of identification processes. Arguably, the idea of reintroducing a National Identity Card Scheme is a response to this rise in concern over the safety of individual identities.

Chapter 4

The fuss about identity cards

Introduction

This chapter will discuss the political and social implications of introducing a National Identity Card Scheme. The history of previous identity card schemes both in the U.K. and in other countries is the first subject for discussion. The next area dealt with in this chapter is the political discourse over the subject of identity cards. Due to political disagreement over the implications for civil liberty implications of introducing an identity card scheme many modern commentaries can often be high polarised either for or against the identity card scheme. The issues raised in the debate over identity cards will be discussed. The goal of this chapter is to illustrate the development of the concept of identity cards and to highlight the current discourse on this subject; this will be achieved through the use of literature from news reports and arguments for and against the introduction of identity cards.

History of ID cards

In 1995, plans were in place to introduce an identity card scheme, and a Green Paper on Identity Cards (1995) was published to invite opinions. A joint response titled *'Identity Cards Revisited'* to this Green Paper came from the Institute for Public Policy Research and JUSTICE, which highlighted previous attempts to introduce identity cards in the United Kingdom and questioned the need for such a scheme and its overall usefulness.

This report describes how earlier attempts have been made to use identity cards in the United Kingdom as far back 1939, when the outbreak of war brought about the creation of the 'National Registration Act'. This act was meant as a mean of efficiently operating the rationing schemes for food and clothing during the war. This act also allowed the police the power to demand to see a person's identity card without any connection to a crime being required. The 'National Registration Act' was eventually repealed in 1953 because of this practice by the police. According to this report, it was a test case in the High Court (in which a motorist refused to show his identity card and was subsequently

arrested) that brought about the end to this form of identity card. In this case, the Lord Chief Justice is quoted as saying:

> "....although the police may have powers, it does not follow that they ought to exercise them on all occasions... it is obvious that the police now, as a matter of routine, demand the production of national registration cards whenever they stop or interrogate a motorist for whatever cause... This Act was passed for security purposes, and not for the purposes for which, apparently, it is now sought to be used... in this country we have always prided ourselves on the good feeling that exists between the police and the public and such action tends to make the public resentful of the acts of the police and inclines them to obstruct them rather than to assist them." (Willcock v Muckle, 1952, 1 KB367, at p. 369 cited in Identity Cards Revisited Report, 1995: 3)

Since 1953, several Conservative and Labour governments have suggested reintroducing an identity card scheme. The arguments have usually focused on the advantages to administrative processes that an identity card would provide. It has been argued that with an ID card the welfare state would run more smoothly. According to *Identity Cards Revisited* (1995) each time the ID card was suggested, the opposition party, be it Labour or Conservative, have argued that the system would be too expensive.

The issue of crime prevention and crime control began to emerge in discourse on identity cards during the mid 1990s. In the 1995 Green Paper on Identity Cards, their role as a means of improving law enforcement and crime prevention was introduced. However according to Davies (1996) the Association of Chief Police Officers (ACPO) were less enthusiastic about the use of identity cards as a tool of crime prevention; they believed that demanding ID cards from the public would erode public relations. Davies notes:

"...the major problem in combating crime is not lack of identification procedures, but difficulties in the gathering of evidence and the pursuit of a prosecution. Indeed, few police or criminologists have been able to advance any evidence whatever that the existence of a card would actually reduce the incidence of crime, or the success of prosecution." (Davies .S, 1996: 5)

However Davies does acknowledge the usefulness of the National DNA database as a means of improving the detection of offenders. Looking at fraud and the usefulness of ID cards in combating fraud, Davies notes that the more an identity card is valued by society the more likely it is that fraudsters will attempt to copy or counterfeit it.
In 1997 when Tony Blair was shadow Home Secretary he argued against the identity card scheme proposed by the then Conservative government. While the 1996 proposal of an identity card was turned down, the latest identity card scheme proposed by the Labour government has gone forward despite a great deal of opposition. Why has this current identity card proposal succeeded where others have not?

The answer is related to the changes that have taken place in society over the last 15 years in particular with regard to identity and national security. To elaborate, in western societies such as the U.K. the culture has changed with regard to identity. Through technology like the internet and the opportunities to express an individual's sense of self on the internet, and medical advances such as gender reassignment procedures, there is more ambiguity available to individuals when it comes to their identity. Even in terms of dress and language it is becoming harder to distinguish things such as a person's class. It can be argued that we have developed into a society that allows for anonymity and greater self determination as to how others perceive us. This trend does have its negative side; on September 11th 2001 terrorist attacks in the United States of America sparked world wide concern over Islamic extremist attacks. This concern over identifying terrorist was joined by concern over illegal immigration and asylum seekers and several high profile instances of identity theft and identity fraud. From 2001 until today we have in a sense been in a perfect storm of moral panic over the identification process. We need to know who the terrorists are, we need to know who is here legally and who is

here illegally and on an individual basis we need reassurance that no one is impersonating us and stealing our bank account details.

The response to this concern came in 2002 with a new call for an identity card scheme. The scheme was originally called the Entitlement Card Scheme and the stated goal was to aid in preventing and detecting crime. This is why the scheme has not been shut down; the idea that the identity card can stop crime has given it the appearances of being more cost effective and justifying what is seen by some as an invasion of privacy.

The entitlement card scheme proposed a new and secure form of ID which would be protected by biometric security. In principle the card would stop illegal immigration by making it impossible to work in the U.K. without one; it would stop benefit cheats by making the identity card a requirement of welfare applications. Ultimately, in principle, the hope was that it would stop terrorists from concealing themselves in the U.K.

Passport security

As the passport office has recently introduced a biometric element to passports there is information here on the ways a biometric system will be used and its usefulness. According to the United Kingdom Passport Service they are introducing the new facial recognition system for passports as a means to improve security around travel documents. One of the reasons for this effort is to support the International Civil Aviation Organisation's efforts to develop international standards for biometrics deployment within travel documents.

ID cards in other countries

In a report for Privacy International by Simon Davies (1996), on the use of identity cards around the world Davies notes that a number of countries have rejected the idea of an identity card, amongst them America, Canada and Sweden. However, European countries such as France, Portugal, and Spain have adopted an identity card scheme. Looking at the use of identity cards around the world, Davies notes that there are a variety of reasons for establishing an identity card system:

> "Race, politics and religion were often at the heart of older ID systems. The threat of insurgents or political extremists, and the exercise of religious discrimination have been all too common as motivation for the establishment of ID systems which would force enemies of the State into registration, or make them vulnerable in the open without proper documents. In Pakistan, the cards are used to enforce a quota system, in China, they are used as a tool of social engineering." (Davies .S, 1996: 1)

When discussing the previous plans to introduce an identity card scheme in the UK in the 1990s Davies notes that this scheme like others introduced in Holland and Australia was intended as a means of improving administrative efficiency and combating fraud in the welfare system. Davies notes that as well as providing improved services and a method of combating identity fraud, the introduction of an identity card also involves an increase in police powers with regard to detaining people and demanding they present their identity card when it is requested by the police.

When considering the issue of identity cards it is important to understand the policy based criticism levelled at previously proposed identity card schemes, namely the issues of cost and the invasion of privacy. As the idea of using an identity card as a means of preventing crime began to emerge it can be argued that people who were pro identity cards finally had a counter argument. The political upside of suggesting identity cards in the 21st century is that they appear to be a means of stopping identity fraud, illegal immigration and terrorism and answer our concerns over deception in the identification process.

Political discourse on ID cards and views of opposition groups

The history of identity cards has often involved heated debate, and the current plans for a National Identity Card Scheme have motivated several different protest groups to speak out against it. The debate surrounding the introduction of the National Identity Card Scheme is an important area to discuss as the debate amongst protest groups and

political parties has raised several important issues about the effect an identity card will have on society in the U.K. The criticisms laid against previously proposed identity card schemes, such as issues of cost and implications for people's civil liberties, have been raised again by politicians and protest groups.

In a study by the London School of Economics the issues of cost were attacked; also, groups such as Liberty, Privacy International and NO2ID have attacked the identity card on the grounds of invasion of privacy. These are important areas of contention that the government has attempted to address with varying degrees of success. Ultimately, however, very few have tried to challenge the identity card on the grounds of whether or not it will work.

The political discourse on whether or not to introduce the identity card has focused on issues of privacy and cost. This discourse has lead to several changes to the National Identity Card Scheme since it was originally proposed. Cost and effects to people's sense of privacy have lead to several changes to the identity card even before it has been introduced. Cost has driven as much of the political discourse as the issue of privacy. There are several elements to the issue of cost; setting up the system, running it, and the cost to the individual. On all three elements there have been differing opinions as to how much the identity card will cost. The cost of setting up the system has been judged to be in the billions and no number is available to determine what the system will cost to run as there is no pre-existing identity card system to compare the U.K. identity card scheme to. By far the most controversial issue of cost is that of the cost to the individual. Some estimates have the cost of the individual identity card at £200 pounds per person and others at £30. The issue of cost to the individual may not have been such a big issue if people had a choice in whether or not to have the card, but one element of the identity card which the government have remained firm on is that it is compulsory to everyone in the U.K.

Another significant effect is the limiting of full access to cards to public sector services only. Originally, the 2002 proposal envisaged the identity card being used throughout society for both public and private sector institutions. The government went so far as to offer access to the National Identity Register to private companies for a fee. The thinking behind this move was that it would help keep the cost of the identity card down. In principle, the more the identity card was used, the better it would be at preventing and detecting crime. However, when these plans were revealed through the media, opponents of the identity card argued that the card's function had crept too far and that its use in all aspects of society would be too invasive. So access to the register was limited to public services only with private companies allowed to verify but not alter the identity card, at a cost, and with the permission of the card holder.

Opposition to the identity card scheme has been voiced not only through media reporting but also on the websites of various civil liberty advocates such as NO2ID, Liberty, Privacy International and Justice Not Vengeance. On these websites, attacks on the identity card scheme often focus on the potential curtailment of civil liberties, the cost of the identity card scheme and issues of personal privacy. The concerns of civil rights campaigners with regard to cost are that by forcing people to pay £35 for an identity card, the government is in effect creating a tax on identity. The director of Liberty Shami Chakrabarti, also indicated that there were implications with regard to the issue of personal privacy and civil liberty. Published on the Liberty website Chakrabarti outlines her opposition to the identity card:

> "My problem as Director of Liberty is that at the height of the so-called War on Terror, when absolute rules like prohibition on torture are compromised by our political rulers, how much harder to defend more subtle and qualified rights like the presumption of privacy from the chilling slogan politics of 'nothing to hide, nothing to fear'." (Chakrabarti .S 2007: 1)

Privacy has been a major issue for opponents of the identity card scheme. They believe that identity cards will undermine societal trust and create a rift between the individual and the state. This issue of creating a rift between the individual and the state is one that brought the old identity card scheme of the 1940s and 50s to an end in the U.K. However, it is worth noting that other countries have identity card schemes for example France Belgium and Spain all have identity cards and there does not appear to be major concerns over infringement of civil liberties or privacy rights being impeded.

It may be that the concerns over the identity card in the U.K are not specifically concerned with the idea of an identity card, rather with the reasoning behind for the identity card, and the justification for the information it requests, and the political motivation for the scheme. Chakrabarti from the human rights advocacy group 'Liberty' argues that:

> "Perhaps when policy is built upon opinion polling rather than principle, these are the inevitable authoritarian results? But I wonder. Support for the intrusive, discriminatory and expensive folly of identity cards in steady decline. The latest bright idea of an information free-for-all within Government with the massive corresponding risks of error and fraud will only exacerbate widening popular concern as to the competence of public administration and who really serves whom." (Chakrabarti .S 2007: 2)

Other organisations who oppose the introduction of the identity card are Justice Not Vengeance (JNV), Stand, NO2ID and Defy ID. According to Justice Not Vengeance (JNV) the aim of the National Identity Card Scheme is not to protect against terrorism or to stop crime, it is rather an instrument to expand state control. In order to promote this view of the identity card, Justice Not Vengeance in 2004 noted the shortcomings of the National Identity Card in its April 2004 Anti War Briefing – *NO ID*. In this briefing, JNV note that identity cards will not stop terrorism or detect terrorists before they attack. This approach is used by many of the anti ID card groups, highlighting the ways that an identity will not work in the way that is intended.

Another approach to opposing the National Identity Card Scheme is to question the further implications of introducing an identity card. Like many groups opposed to the introduction of the identity card, Defy ID highlight the role of the National Identity Register and how this may be as much a risk to civil liberties as the actual identity card.

> "The ability to check your identity against your entry in the National Identity Register will not just be available to the Immigration Service and the Police but also to 'providers of public services and private sector organisations {e.g. employers, banks, credit reference agencies, libraries, dentists, utilities companies, student loans company etc}. The ID card bill includes a power which in theory could force 'any person' to provide information about you for background checks." (Defy-ID 2004-05: 1-2)

Defy-ID also note that the government's claim that the identity card will prevent terrorists from obtaining access to services in the U.K. without the ID card will mean that ordinary citizens will also be under the same constraints.

Another group opposed to the identity card scheme is NO2ID; this organisation campaigns against the Identity Card Act. Like Defy-ID, NO2ID have highlighted the downside of introducing ID cards with regard to preventing crimes such as illegal immigration, benefit fraud and identity fraud. On the subject of identity fraud NO2ID note that:

> "Both Australia and the USA have far worse problems of identity theft than Britain, precisely because of a general reliance on a single reference source. Costs usually cited for of identity-related crime here include much fraud not susceptible to an ID system. Nominally 'secure', trusted, ID is more useful to the fraudster. The Home Office has not explained how it will stop registration by identity thieves in the personae of innocent others. Coherent collection of all

> sensitive personal data by government, and its easy transmission between departments, will create vast new opportunities for data-theft." (NO2ID, 2007: 2)

Trevor Mendham is a writer on the subject of civil liberties who is opposed to identity cards and is a coordinator in Scotland for NO2ID. Several questions on the subject of civil liberties and the National Identity Card Scheme and the National Identity Register were posed to Mendham:

> "1} What is it that the national register does that other government and private
> databases don't do that makes it such a threat to civil liberties?
>
> 1} It's the arbitrary invasion of privacy. One big, central database containing all sorts of information about us. In particular the "audit trail" means that the government will have a record of every time our card is checked against the central database. This is defined in para 9 of Schedule 1:
> http://www.opsi.gov.uk/ACTS/acts2006/60015--b.htm#sch1
> And we can't "opt out".
>
> 2} Given the way our society works what is the problem with having a national register? We already freely give out masses of information about ourselves to private organisations and government agencies. To play a bit of devils advocate
> where is the issue of liberty? To be a part of society you have to be recognised by society won't a national register merely formalise what we do every day? If being unknown to the state is a liberty then we all give it up quite early on in life don't we?
>
> 2} You used one vital word: "freely". For example I have chosen NOT to use supermarket loyalty cards. I with have no choice about the NIR

and ID Card. In addition the existing databases are all "information silos". Government departments -and private companies - know what they need to know and no more. The NIR turns this principle on it's head and says "We'll record everything we can just in case it's useful".
Yes, there are times when we must give up information for society to function, I accept that. But currently they are considered necessary exceptions rather than the general rule.

3} Why is privacy more important than security? Is it better to have privacy and crimes like illegal immigration or is it better to have no privacy but the reassurance that the state knows who every member of society is and can verify that information?

There is no evidence that ID Cards will actually stop these crimes and give us any significant extra security. Many countries have compulsory ID cards and still suffer from illegal immigration, crime and terrorism.
Privacy is essential for a free society. Without privacy it's very difficult to be different, to be an individual. Or, in political terms, a dissident.
That's why privacy is included in article 12 of the Universal Declaration of Human Rights:
http://www.unhchr.ch/udhr/lang/eng.htm
We're supposedly fighting the terrorists in order to preserve our way of life. If we give up that way of life then they've won." (Mendham .T, 2006: 1 of 1 see appendix 4 for original email)

Opposition groups, when discussing identity cards, often promote public protest by petitions against the introduction of the identity card and by public demonstrations, and their attack on the cards often focuses both on the identity card's ability to succeed and the possible negative implications of what might happen if the scheme were to be

introduced. Discussion of the impact of identity cards can be found in many of the major newspapers where members of protest groups or journalists often speculate about the potential impact of the cards.

An example is an article in the Sunday Mail by Simon Davies (2004), entitled *'Do you want MI5 to know your medical details? They soon will – and it will cost you £35'*. Simon Davies is the head of Privacy International, an organisation that is very vocal in its resistance to identity cards, citing the human rights and civil liberties that will be infringed or denied by the introduction of a National Identity Card Scheme. In his article Davies discusses how the identity card is a means of creating a surveillance society that will deny people the right to privacy rather than protect them or make their lives easier:

> "This is not a plan to help citizens beat the problem of wallets over stuffed with cards. It is a surveillance system that will prove a disgrace to democracy"
> (Davies .S, 2004: 13)

Davies highlights the creation of a variety of offences that accompany the present identity card scheme. According to Davies, there are a number of fines that accompany the new identity card scheme. These fines cover things such as failure to report changes in personal circumstances, or providing false information which can be dealt with by a fine of a £1000 or up to two years in prison.

Along with the new identity card, there will be the introduction of a National Identity Register where information on every person enrolled in the system will be stored. In the bill for the identity card scheme, the Home Secretary has the power to divulge identification information to a range of government agencies. According to Davies there is also legislation giving the Home Secretary the power to compel people to register and to register people without their consent.

> "So we shall all be compelled constantly to provide personal information to government, which will then pass the data on to any organisation it chooses.

> Tough luck if you don't feel comfortable with the police knowing your every detail. Or if you don't like the idea of the Inland Revenue knowing your medical records." (Davies .S, 2004: 13)

Aside from the impact of an identity card scheme on society, Davies also discusses the crime of identity fraud and how an identity card would influence this type of crime. Davies (1996) argues that the causes of fraud are situated in human and organisational issues rather than a lack of technology. Looking at benefit agencies from around the world and their work on the causes of fraud, Davies argues that the three most common forms of fraud are-

- "False declaration, or non declaration, of income and assets {problems which are also components of non declaration of income for tax}
- Criminal acquisition of multiple benefits using false identification
- More conventional fraud and theft of benefit payments" (Davies .S, 1996: 6)

Therefore the introduction of an identity card scheme would have minimal effect on the levels of fraud. With regard to illegal immigration Davies argues that identity cards will help in combating illegal immigration if the police and other services involved in investigating illegal immigration are given broad powers to stop and demand identity cards from people. According to Davies, these powers could either be used on everyone, resulting in a culture of constant identity checking; or by targeting minority groups or communities. With either alternatives, questions of civil liberties are raised.

On the subject of police powers, Davies highlights that in many countries there have been claims of abuse made against the police with regard to demanding identity cards. In these cases of abuse, the failure to produce an identity card when demanded has also lead to people being detained:

> "While it is true that cards containing non sensitive data are less likely to be used against the individual, cards are often alleged to be the vehicle for discriminatory practices." (Davies .S, 1996: 8)

Davies goes on to argue that by their very nature identity cards are discriminatory as they will often be used against minority groups to combat illegal immigration. According to Davies if there were no discrimination in the use of identity cards, this would result in random checks of the entire population which would prove to be politically unacceptable.

News reports on identity cards also include discussion of the financial implications of introducing a National Identity Card Scheme. In an article for BBC News (2004), the use of civil financial fines for people who do not register for the new identity card scheme is reported. These fines may be as much as £2500. The decision on making identity cards compulsory will go on until 2013 according to this article. The reason put forward by the government for making identity cards compulsory is to avoid terrorist attacks and to improve standards of detection with regard to crimes such as Identity fraud, people smuggling and illegal employment. The use of Britain for health tourism and abuse of the welfare system is also a concern. Concerns have been raised by opposition parties and civil rights campaign groups. For the opposition parties the concern is about the implementation of this scheme and its cost:

> "Liberal Democrat home affairs spokesman Mark Oaten said: 'I would much rather see the £3bn that's going to be incurred in looking at better intelligence'. Shadow Home Secretary David Davis said Tories were sceptical about the home office's ability to successfully introduce ID cards – but added the idea must be looked at 'carefully'. 'The practical problems in the way of ID cards are immense.' "If a scheme can overcome these problems without sacrificing civil liberties, ID cards should be introduced soon- not in ten years time. The terrorist threat is real, and is here today," Mr Davis said." (BBC News, 2004: 2-3)

News reports also cover the issue of the social implications of introducing an identity card and the political nature of the decision to introduce such a scheme. The reporting of the Queens speech by the Independent in 2004 highlights the criticisms levelled at Labour for introducing the identity card scheme. Morris (2004) notes that:

> "Mr Blunkett has faced accusations he is using the threat of terrorism to give impetus to his pet project. Many Labour MPs – including cabinet members- are worried about giving the state too much power; the Commission for Racial Equality has warned that ID Cards could inflame racial tensions. Critics point out that an identity system was in operation at the scene of the Madrid bombings." (Morris .N 2004: 1)

In this report, Morris highlights the claims that then Prime Minister Tony Blair and David Blunkett were at the time scaremongering in order to gain during elections. The report also looks at the introduction of new laws regarding drugs, organised crime, anti social behaviour and terrorism. Since the Queen's speech there has been a great deal of activity with regard to identity card legislation. In a report by Michael White, David Hencke and Alan Travis (2005) for the Guardian, it is noted that bills such as the identity card bill would be sacrificed because of the approach of an election in May 2005 and difficulty in gaining support from the Conservatives and the Liberal Democrats.

> "'The Tories don't know where they are on the bill so the easiest thing to do would be to stop it,' the minister said, in reference to Conservative flip flops on the issue. They abstained on the third reading." (White .M, Hencke .D, Travis .A, 2005: 2)

In a report by Andrew Grice for the Independent the political strategies used by both the Labour government and the Conservatives are discussed. According to Grice-

> "Labour is preparing to blame the Tories for the delay, accusing them of weakening the fight against terrorism. This is increasing the pressure on the Opposition not to scupper the Prevention of Terrorism Bill, which would allow the Home Secretary to put suspects under house arrest. Senior Tories fear that if they halt both measures, it would make it easier for Labour to portray them as 'soft' on crime. 'We can block one of the Bills but not both,'" (Grice .A, 2005: 6)

The political battles over the introduction of the identity card have continued as the date for the introduction of the identity card scheme approaches. These reports on the progress of the bill to introduce an identity card to Britain show that this decision is not being made in a vacuum, it is in part linked to new anti-terrorism legislation and the public appearance of the political parties with regard to crime. But as the advocates for the identity card bill begin to highlight its usefulness, so too have its critics challenged the wisdom of even introducing an identity card scheme.

The Conservative and Liberal Democratic parties have outlined, on their websites and in statements to the general public, their objections to the introduction of an identity card scheme. The Conservatives, while previously suggesting the introduction of identity cards have denounced the current identity card scheme. According to the Conservative party website, if the Conservatives were to win the next election they would immediately scrap the Identity Card Scheme. Also on the Conservative Party website is an outline of the reasons why the identity card is not a good idea and what the Conservatives would do instead. The website states that identity cards would not succeed in preventing terrorism, illegal immigration, identity fraud or human trafficking. The website also notes the cost of the system at £20 billion and the cost to the individual for an identity card at £93 as reasons not to introduce the system. It states:

"ID cards will cost each person £93: According to government estimates, you will pay at least £93 for a combined ID card and passport package but, given this government's appalling record of implementing IT projects, this figure is likely to go up. Also, if your ID card is stolen, or you lose it, you'll have to pay £30 for a replacement. If you change your name when you get married, you'll have to pay for a new ID card. If one of your relatives dies and you forget to return their ID card, you could be fined £1,000." (Conservative Party, 2007 see appendix 5 for original email)

Aside from the shortcomings of the system and its costs, the Conservatives also criticise the identity cards on the grounds of the government's success rate with regard to implementing large scale information technology projects and the invasion of privacy the identity card will constitute. The alternative to identity cards, according to the Conservatives, is to create more prison places, more drug rehabilitation facilities in prisons, and a boarder police force as a means of detecting and preventing illegal immigration and the movement of terrorists into the U.K.

Of all the political parties represented in parliament, the one party to have opposed the identity card scheme most consistently is the Liberal Democrat party. Not only does this party oppose the identity card, it has also suggested an alternative to the identity card scheme. Mathew Hanney policy researcher to Nick Clegg MP and Liberal Democrat Shadow Home Secretary has written:

"Below I have outlined the Liberal Democrat position on the points you raised:
1. How do you think the proposed ID card system will fare as a means of preventing crime?

1. The government has yet to offer any conclusive proof that ID cards prove beneficial in the prevention of crime. Indeed, it is possible that they would lead to an increase in some crimes, such as fraud. Though the government have insisted that these cards would be impossible to forge, this claim is somewhat

implausible. ID cards will become the "holy grail" to fraudsters and terrorists, and with ever developing technology it seems unlikely that we can be definite about their security.

2. How do you think the proposed Id card system will fare as a means of

detecting -

- criminals
- terrorists
- illegal immigrants

2. There has been no positive link established between the introduction of ID cards and a reduction in crime or terrorism. We are sceptical about the idea that ID cards would reduce illegal immigration. Employers in industries with a high level of illegal immigrant labour are already required to check identity documents before employing someone. It is the blatant disregard to this procedure which needs to be tackled (via inspections), rather than the question of ID cards.

3. What alternative to id cards - with regard to preventing crimes such as id fraud, illegal immigration and terrorism does the Liberal Democrats propose?

3. Obviously our alternative policies in these wide ranging areas are complex, and I recommend our website (www.libdems.org.uk) for more in-depth information. But our top policies are: with the money saved from not implementing the ID card scheme, we would put 10,000 more police on the street along with investment in extra equipment and new technology.

We do support biometrics passports, believing these would be more effective at tackling cross border fraud, terrorism and illegal immigration. We also propose to establish a National Border Agency, bringing together officers from customs, police and immigration who currently have overlapping responsibilities. We

back the use of phone tapping and other 'intercept communications' evidence in court against terrorist suspects.

4. What do you think the social implications of having an id card in the U.K. will be? How will it change our lives?

4. Introducing ID cards in Britain would have a huge social impact. Britain is a country with a strong tradition of civil liberties. Also, unlike every other country with ID cards, the UK does not have a written constitution to protect its citizens. With the relationship between state and citizen not properly defined by law, the risks of an abuse of state power are greater. ID cards will unquestionably tilt the balance of power in the UK away from individuals and towards the government.

The cards could also lead to a culture of mistrust, for example ID cards may be required to keep an appointment with a GP. It may also lead to a growth in discrimination. An increase in racial and ethnic tensions as a result of the introduction of ID card is regrettably an all too likely occurrence.

5. What difficulties do you think the government will face in trying to implement this system?

5. The possible difficulties involved in implementing a scheme on such a large scale are numerous. Yet such errors will have serious implications such as the withholding of benefits and the denial of services.

The government has a woeful history of organising large scale IT projects, with large scale overspending practically the norm. ID cards will be the largest scale public sector IT project undertaken, and considering the failure of smaller government projects such as in the Police Service, Courts Service, CSA and NHS it is not surprisingly that we feel a lack of confidence in the prospects for this scheme.

6. From my research so far I have determined that a lot of people want the id card and think that it is a good idea (Recent Yougov poll) - what is it they are not considering or are unaware of?

6. We are sceptical of how reliable any poll finding can be, since the Government still has not come clean about the real cost of this scheme or its draw backs." (Hanney .M, 2006: 1-2 see appendix 6 for original email)

Most opposition to the identity card scheme presented by political parties has addressed the practical shortcomings of the identity card, but some parties have also addressed the implications for civil liberties of the scheme. One of the main alternatives discussed has been the introduction of a border police force. This idea has been suggested by both the Conservatives and Liberal Democrats as a means of improving security against illegal immigration and terrorism. Curiously, however, neither the Conservatives nor the Liberal Democrats have suggested a policy to directly confront the rise in identity fraud. While the Liberal Democrats have suggested recruiting 10,000 more police officers, these are not directly intended for investigation of fraud. Equally, while the Conservatives have suggested a solution to illegal immigration and terrorism, they have not presented a solution to identity fraud. Both parties, rather than addressing the 'unholy trinity' of 21st crime (terrorism, illegal immigration and identity fraud) have opted to focus on the crimes of terrorism and illegal immigration. While this may decrease the overall numbers of cases of identity fraud in the U.K. it will not address identity fraud committed for profit or over the internet.

It can be argued that while the debate over the introduction of an identity card scheme has raised several important issues for the study of identity cards, there may also be a degree of bias in the discourse provided by politicians and protest groups. The debate over the introduction of identity cards can be seen as one facet of a larger debate over the expansion of state powers. With increased concern over terrorism the debate about how much power the state should have to monitor and detain people has increased since

the attacks in New York in 2001. The protest groups discussed above not only oppose the introduction of identity cards but are also vocal opponents of the expansion of police powers. As such, their views on identity cards may be seen as keeping to a more general perspective of the role of the state. Equally, the views expressed by politicians against identity cards may also be seen as keeping to some general political stance on the role of the state. Historically both the Conservative and Labour parties while in power have suggested an identity card scheme; equally both parties when not in power have criticised the government for suggesting the introduction of an identity card scheme. As such, the views of political parties and protest groups are useful but also open to a degree of bias.

Conclusion

The history of identity card schemes in the U.K. shows us that while the U.K has previously accepted and used an identity card there has still been controversy and criticism attached to any attempt to re-introduce an identity card scheme to the U.K. The current reintroduction of the identity card to the U.K., however, faces an even more heated debate. While older identity card schemes emphasised their usefulness as a tool for improving administrative processes, the current identity card scheme is intended as a tool for crime prevention and detection.

It can be argued that this shift in purpose for an identity card is due to increased concern over terrorism, illegal immigration and identity fraud. However, in the process of trying to make society safer by stopping identity thieves through identity cards, critics claim that Britain is in danger of becoming a surveillance society. It is argued that by introducing an identity card scheme the government will focus more on monitoring everyone than stopping those involved in criminal activity.

While most of the discourse between supporters of the identity card scheme and its critics focuses on this question of a surveillance society, less is said about the potential of identity cards to prevent identity fraud. The goal of this study is to discuss how identity cards might impact the activities of the minority of people who use identity

fraud, rather than the majority of people who do not. To achieve this goal, this study has explored the use of simulated identity theft as a method of researching identity fraud. This study has also used analysis and discussion over the internet to research the crime of identity fraud and the use of identity cards. In the next chapter the methodological approach of this study will be discussed.

THE MICHELLE BROWN CASE

This case from America is an important example of identity fraud as it highlighted the dangers people faced and the lack of legislation to protect victims.

Below is the verbal testimony of Michelle Brown, given to the Senate Committee Hearing on the Judiciary Subcommittee on Technology, Terrorism and Government Information "Identity Theft: How to Protect and Restore Your Good Name" (July 12, 2000)

Verbal Testimony by Michelle Brown

Mr. Chairman and Members of the Committee,

I am pleased to be in your presence today and I genuinely thank you for the opportunity to elevate the invasive crime known as identity theft. This is a topic that I am unfortunately, intimately familiar with.

My name is Michelle Brown. I am 29 years old and have been working in the disciplined field of international banking for the last 7 years. I am an ambitious and hard-working individual; I'm certain that I am much like any of your cousins, your nieces, your daughters. I believe that I strongly represent any average, respectable citizen of the United States. However, there is one clear-cut issue that separates me from nearly the rest of the population: I have lived and breathed the nightmare of identity theft. I will tell you first-hand, this is a devastation beyond any outsiders' comprehension, a nearly unbearable burden that no one should ever have to suffer.

Imagine establishing credit at age 17, and building a perfect credit profile over the next 11 years. Imagine working consistently since age 15, helping to finance your education at an accredited University to advance your future success in life. Imagine never having been in trouble with the law. Imagine the violation you would internalize as you realize some vile individual you have never met nor wronged, has taken everything you have built-up from scratch to grossly use and abuse your good name and unblemished credit profile.

That's precisely what happened to me. I discovered this new blackened reality on January 12, 1999, when a Bank of America representative called me inquiring

about the first payment on a brand new truck, which had been purchased just the previous month. I immediately placed fraud alerts on my credit reports, cancelled all credit cards, and even placed a fraud alert on my Driver's License number. From that day forward, I unearthed the trail of this menace's impersonation and attempted to work with the current faulty system to protect myself from any further abuse. **The system clearly failed me.**

To summarize, over a year and a half from January 1998 through July 1999, one individual impersonated me to procure over $50,000 in goods and services. Not only did she damage my credit, but she escalated her crimes to a level that I never truly expected: she engaged in drug trafficking. The crime resulted in my erroneous arrest record, a warrant out for my arrest, and eventually, a prison record when she was booked under my name as an inmate in the Chicago Federal Prison.

The impersonation began with the perpetrator's theft of my rental application from my landlord's property management office in January 1998. Immediately, the perpetrator set up cellular service, followed by residential telephone and other utility services, attempted to obtain timeshare financing and department store credit cards, purchased a $32,000 truck, had nearly $5,000 worth of liposuction performed to her body, and even rented properties in my name including signing a year lease. Not only did this person defraud the Department of Motor Vehicles in obtaining a duplicate drivers' license (with my name and number) in October 1998, but she even presented herself as me with this identification to the DEA and before a federal judge when she was caught trafficking 3,000 pounds of marijuana in May 1999.

She remained a fugitive for almost 6 months while still assuming my name-- and was finally turned in by an acquaintance in July 1999.

Months later - in September 1999 - I was stopped at LAX's Customs after returning from a vacation in Mexico (after she was already in prison). While I explained my innocence to several agents in a stream of tears, and as I attempted to clearly distinguish this Michelle Brown from the "other Michelle Brown" with a criminal record, I was blatantly treated with strong suspicion. I was, as is

typical for an identity fraud victim, guilty until proven innocent. I was finally let go after an hour, after the police were called to vouch for me. This situation reinforced my fear that I may be wrongly identified as the criminal, which could end up with my arrest, or worse yet, being taken into custody to serve time in jail. After having seen so many inefficiencies and blatant errors in the system, I feel no assurance nor can I receive any concrete evidence from authorities that this type of insane mix-up would **never happen again.**

It was tormenting to know someone was in essence living the good life at my expense, and I was left in the dust with the taxing chore of proving my innocence. The restoration of my credit and my good name was a seemingly never-ending process. I was forced to make literally thousands of phone calls, fill out various forms, submit all sorts of documents, and have many documents notarized. Without a doubt, I was entirely consumed with the whole painstaking process. I gained nothing from putting over 500 hours into the chore of restoration; all in all, it was an exhausting waste of a good person's time and a massive drain on my life and energy. At one point, I even feared my safety after I learned that the perpetrator had previously been linked with a convicted murderer. The whole identity fraud experience was, by far, the darkest, most challenging and terrifying chapter of my life.

I faced many difficulties in clearing my name, and I still face the fear that I will forever be linked with the perpetrator's criminal record. I have encountered widespread inefficiency and general insensitivity at nearly every turn, and know that there are most definitely not enough dedicated resources and governmental authorities to assist victims and to simplify the burden on the innocent's life. Clearly changes need to be made. The Government not only needs to promote initiatives to shorten and simplify restoration of one's name and credit, but also to facilitate early detection and termination of an abused name, and most importantly, to deter criminals from the lure of such an easy crime by enforcing swift and severe punishment.

I think that Senator Feinstein's Identity Theft Prevention Act of 2000 is definitely a positive initiative and will put the legislation in the right direction to

fight this crime. I support the two corresponding bills and recommend the enforcement of such initiatives.

I came here today because I feel responsible to limit the abuse of other innocent's names and their lives. I know how terribly tormenting it is to be a victim. I am living proof that identity theft is a very real crime, with very real victims, and true life-altering consequences. It's astounding that my life-long discipline to be a law abiding citizen, and to have the diligence to establish perfect credit, was reversed so easily, so quickly, simply because I represent the perfect victim in a criminal's eyes. This crime is clearly on the rise, and no one at this time is completely protected from becoming the next victim.

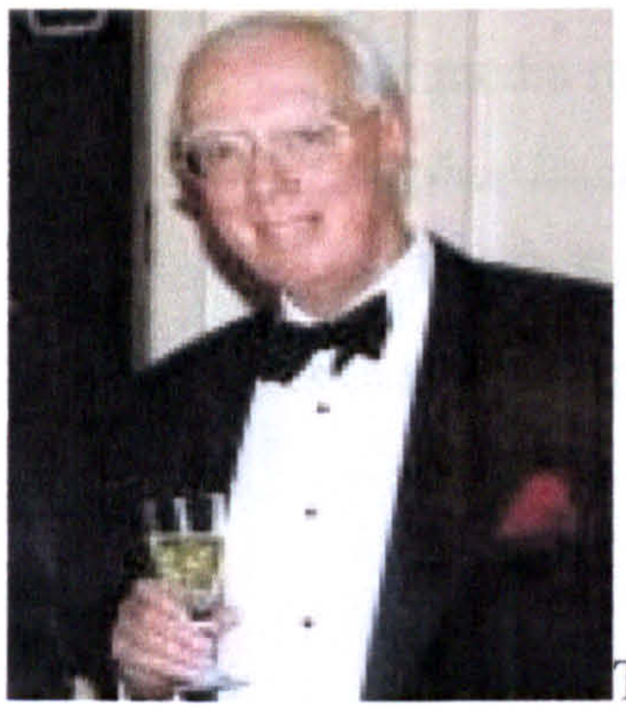
I realize the scenario of becoming an identity fraud victim seems entirely far-fetched and implausible to many of you. I know the feeling. I was once in your shoes.

I thank you for your time and for the opportunity to present my story and views today. I hope it is clear now that many changes need to effected to the current system to combat this crime and protect victims. This fact is crystal clear in my mind.

(Brown 2000: 1-5)

THE DEREK BOND CASE

Derek Lloyd Sykes (BBC News 2003: 1)



The Real Derek Bond (BBC News, 2005: 1)

One of the most famous cases of identity fraud in recent years was the case of 72 year old Derek Bond. What makes Mr Bond's case so noteworthy is that it was the first high profile case of identity fraud involving a U.K. citizen. This case prompted the rise in concern with regard to identity fraud in the U.K. and showed in dramatic fashion the dangers of identity fraud to the general public.

Derek Bond was arrested in South Africa in January 2003, after a warrant for his arrest was issued by the American Federal Bureau of Investigation (F.B.I.). Bond was placed in a South African jail for three weeks, before it was revealed that he was not the man the F.B.I. was looking for. The man the F.B.I. was really looking for was a 72 year old Briton called Derek Lloyd Sykes who was living in America and using Bond's identity. Using Mr Bond's identity, Sykes had participated in a telemarketing scheme with two other men in Houston Texas which had stolen the equivalent of three million pounds during the 1990s. According to Allison (2003) it is estimated that Sykes had been using Bond's identity since 1989. Using Bond's identity Sykes was indicted in 1999 of 22 charges of money laundering, wire fraud and transporting stolen property. Based on this indictment, the F.B.I. issued a warrant for the arrest of Derek Bond, unaware that the

man the F.B.I. was seeking was not Derek Bond. This lead to South African Police in Durban arresting Derek Bond on 6 February 2003; based on this mistake, Derek Bond was imprisoned for 20 days. When the F.B.I. finally caught Sykes, they found he was using another false identity: Robert James Grant, and that he had used this identity for three years. After Sykes was caught, Derek Bond was released.

The case of Derek Bond is important in terms of publicising identity fraud in the U.K. While subsequent media reporting, up until the case of Charles Stopford (otherwise known as Christopher Buckingham), focused on internet based financially motivated fraud, the case of Derek Bond was the first high profile case of identity fraud in the U.K. and illustrates in many respects the worst case scenario for victims of this type of crime.

THE CHRISTOPHER BUCKINGHAM CASE


Charles Albert Stopford (BBC News, 2006: 1)

Aside from the 2003 case of Derek Bond, the most well known and arguably shocking case of identity fraud in the U.K. is the 2005 case of Charles Albert Stopford and his impersonation of Christopher Buckingham. While the case of Derek Bond was instrumental in displaying what many would consider the worst case scenario in terms of identity fraud, the discovery of Stopford's impersonation showed how prolonged and invasive an impersonation could be. Stopford had been impersonating Buckingham for 23 years, and in that time he had married as Buckingham had two children and worked as a computer consultant. In 2006, in a report for ABC news, Martin Bashir and Rob Wallace referred to Stopford as 'The Great American Impostor'. What makes Stopford's impersonation so noteworthy was the length and depth of his impersonation. Stopford had for 23 years abandoned his real identity in favour of being known as Christopher Buckingham. This form of identity fraud is known as wholesale assumption (see chapter 8 for more on wholesale assumption).

Charles Albert Stopford was born in Orlando Florida in 1963, the eldest of nine children. It is reported by Bashir and Wallace that as a child Stopford was fond of play acting, and in his youth there were two events which may have been influential in his subsequent decision to take up a new identity. Firstly, when he was in his teens, Stopford's parent's divorced, leaving Stopford feeling deeply humiliated and prompting him to leave home. Secondly, it is reported by Bashir and Wallace that in his youth Stopford had blown up a man's car with a pipe bomb. The man was a manager at a Burger King who had fired one of Stopford's friends. After this incident, Stopford was

arrested and prosecuted for the bombing. Soon after this, Stopford left America for Europe and the U.K.

In the U.K., Stopford began implementing his plan to become someone else. The first step was to obtain a new identity, and Stopford chose to use the identity of a dead child called Christopher Buckingham who was born towards the end of 1962 and died several months later in 1963. Stopford found Buckingham's identity by visiting the archive of Births, Deaths and Marriages. According to Stopford, he chose Buckingham's identity for the following reasons:

> "'There was a very, very short time between birth and death.' Buckingham said. 'There would be very little registration, if any registration, with doctors. There would be no state documents & A clean state.'" (Stopford cited in Bashir .M, Wallace .R, 2006: 3)

Along with Buckingham's birth certificate, Stopford accumulated other forms of identification including a National Insurance number and a British passport. In terms of identification, both of these forms of identification are crucial: the National Insurance number allowed Stopford to work in the U.K., and the passport gave him the appearance of a genuine U.K. citizen. According to Stopford:

> "It's like the food chain. You have to use smaller documents to create bigger documents, and those bigger documents then create even larger documents..." (Stopford cited in Bashir .M, Wallace .R, 2006: 3)

In the 23 years that Stopford impersonated Christopher Buckingham, he was able to obtain all the documentation Buckingham would have had if he had lived. In terms of paper proof, Stopford was Buckingham.

While in more short term, financially motivated identity fraud there is often no attempt to embellish the nature of the identity, in the case of Stopford's identity fraud he had to develop a history for the Buckingham identity. According to Stopford, Christopher Buckingham was the only son of Lord Edward Buckingham. His father had been a diplomat in Egypt who, along with Buckingham's mother, had died in a plane crash in 1982. Aside from his family, Stopford also fabricated an education at Harrow and Cambridge University. He furthermore claimed that he was a Lord. In 1984, Buckingham visited West Germany and while staying there met Jody Doe, a 19 year old student from Canada. Several months after their meeting, they married and had two children; both his wife and his children believed Stopford was Buckingham. It was not until 2005 that the deception came to an end.

In 2005 Stopford was travelling from France to the U.K. using the Calais–Dover ferry crossing. While in Calais, Stopford's Buckingham passport was checked by U.K. immigration officials who were stationed there and Stopford's impersonation was discovered. After a 10 month long investigation, Stopford appeared in court still claiming to be Buckingham and refusing to reveal his true identity. He pleaded guilty to falsifying his passport records and was given a 22 month jail sentence.

During his imprisonment, Stopford refused to reveal his true identity even to his children. It was not until his daughter Lindsey began using MySpace to find her fathers family that Stopford's identity was revealed. In the time between the revelation of Stopford's impersonation and discovery of his true identity, several theories were put forward about who Stopford was. Some believed he was a cold war era spy who had continued to live on in the U.K.

Currently, Stopford is living in Zurich and he still uses the name of Christopher Buckingham. When interviewed during the documentary 'Identity Fraud - Outnumbered' (April 3 2008), Stopford explained how he now had a prison ID card with the name Christopher Buckingham and how that further helped to prove his claim to be Christopher Buckingham.

As stated earlier Bashir and Wallace (2006) refer to Stopford as the 'Great American Impostor', and go on to describe him as the most successful hoaxer on record. Arguably, his 23 year impersonation was a thorough and elaborate deception, but it can also be argued that Stopford benefitted from a system which was unable to stop or detect his activities.

Looking at the history of impersonation it is possible to see several men and women who have at least equalled Stopford's exploits and in some cases exceeded even his 23 year impersonation (see chapter 6). The importance of the Stopford case is that it shows how concern over false identity has developed in recent years. It could be argued that Stopford's impersonation might have continued undetected, if it had not been for changes in the way identities are monitored and recorded identities and concern over terrorism and illegal immigration.

CHAPTER 5

Research Methodology

Introduction

The purpose of this study is to establish what identity theft and identity fraud are and how they might be affected by the introduction of an identity card. This chapter will examine various methods of gathering information and researching the subjects of identity fraud and identity cards. The approach taken (in this study) has been to research noteworthy cases of identity theft and identity fraud from the U.K. and elsewhere. These cases have been used to develop an understanding not only of what identity theft and identity fraud are, but also how they are carried out. In considering what is involved in identity theft and identity fraud, it was also considered worthwhile to carry out a thought *(Gedanken)* experiment regarding simulated identity theft, which will be discussed later in the chapter.

The second part of the study involved researching the National Identity Card Scheme through government reports and literature from opposition groups. This proved to be a challenging task, as discourse on the nature and use of the identity card scheme is still open to debate and alteration. This means that when trying to answer the question about what impact an identity card scheme would have on identity theft, it is necessary to take into account factors which have modified and influenced the debate on identity cards.

In studying identity theft, identity fraud and the National Identity Card Scheme, researching through the internet became a valuable approach. Using the internet it was possible to contact people and organisations with experience of each of the subjects, in particular experience of identity theft and fraud. Accessing these people through the internet it was possible to download literature on the subjects which may have been harder to obtain by other means. In this study the internet proved to be a valuable resource and its use is also discussed further in this chapter.

Simulated identity theft as a means of research

The goal of this study is to understand how the process of committing identity fraud might be influenced by the presence of a National Identity Card Scheme. In order to explore this, an explanation is necessary as to how identity theft and fraud is committed now, in the absence of an identity card. Therefore some thought was given as to how a person could steal an identity – what techniques can be used to gather information on people and how such information can be used. This developed into a mental experiment on how identity theft occurs. The experiment was never intended to go past the theoretical stage, since doing this would raise a range of ethical and legal questions, but was performed in order to analyse potential issues. Initially this thought experiment was seen as a means of outlining the different sources of information on a person's identity. But, over time, thought was also given to the ethical, legal and practical issues associated with committing identity theft. After developing an understanding of how an identity can be stolen these thoughts were organised into a 'model' of how to steal an identity, referred to in this study as simulated identity theft.

In discussing simulated identity theft, the goal is twofold: firstly, to examine how a person's identity might be stolen in a genuine instance of identity theft; secondly the simulation also raises issues of how an identity might be treated in an attempt to simulate identity theft by academic researchers. When first constructing the simulation, no thought had been given as to who might be administering the simulation. In effect, the simulator was in no way different from a genuine identity thief. This would provide a sense of the different techniques of stealing an identity. But upon further thought, it was decided that not distinguishing between an academic simulation of identity theft and a genuine attempt to steal an identity would deny the opportunity to consider ethical issues associated with academic research which would be useful to the further discussion of identity, issues of privacy and control in the identification process. Arguably inherent in both the discussion of identity theft and identity cards is the issue of who is in control of a person's identity and the process of identification. The experiences of victims of identity theft are discussed in chapter 8 of this thesis; and in all of these cases, the root problem is a loss of control over the individual's identity due to a

loss of control over personal information. Equally, concern over loss of privacy associated with the discussion of the identity card is in a sense a discussion of who should have control over the identification process.

In order to examine these issues of control of an identity the simulation presented here represents thoughts on how an *academic researcher* might adopt a new identity rather than how an *identity thief* might steal an identity. This allows for consideration of ethical and legal issues associated with taking over a research subject's identity. The following section examines how an identity might be stolen as part of a study of an academic study of identity theft in relation to

- previous attempts to use simulated identity theft
- what ethical and legal considerations must be taken into account – How do we determine if and when an identity is stolen
- how an identity might be stolen

Thought was also given as to whether or not an identity could be stolen without victimising the genuine identity holder. In developing simulated identity theft, thought was also given as to whether or not it is possible to avoid defrauding any organisations in society, while at the same time testing their ability to detect identity fraud. The practices of 'ethical hackers' were considered as an example of simulating a crime in order to test security. In order to counter the threat of online attacks, some organisations such as banks and online companies have begun employing 'ethical hackers' to test the security of their IT systems and new web based applications. According to Vyahare (2007) ethical hackers (also known as White Hat hackers) are described thus:

"An ethical hacker is permitted to hack computer systems or networks and he tries his best to hack it. Now the question arises – why? An obvious answer to this is that unless there is an understanding of what's insecure in our system or network, we won't be able to protect it. An ethical hacker provides with vulnerabilities or loop holes in the system or network through extensive use of

various hacking techniques. These vulnerabilities and flaws are then generally corrected through corrective and preventive measures." (Vyavhare .A, 2007: 1)

Ethical hackers use the same techniques as criminal hackers (sometimes referred to as crackers) to attack networks, but the intention in conducting the attack is the exact opposite. The issue of the illegality and harm associated with identity theft can at times be debatable. As discussed in chapter 8 some cases of identity theft and fraud can be prolonged affairs with the victims remaining unaware of the activities of the identity thieves. Equally, in cases of wholesale assumption (such as the case of Charles Stopford) where the identity thief fully adopts the identity of the victim, the issue of harm can also be hard to establish as the identity thief in this instance seeks in most respects to appear to be a law abiding citizen, upholding obligations to organisations within society.

Previous attempts to use simulated identity theft

In this study simulated identity theft is used only as a thought experiment. However, there have been occasions when people have attempted to research identity theft and fraud through practical examples or exercises. Exercises which could be described as examples of simulated identity theft have been conducted by journalists during investigations of identity fraud, and in governmental investigations into identity theft in America.

In 2003 in an investigation for the programme BBC *Kenyon Confronts,* the presenter of the programme obtained a driver's licence in the name of the then Home Secretary- David Blunkett. During this investigation Kenyon was also able to obtain the identifying documents of Frederick Forsyth the author of 'The Day of the Jackal' a book noteworthy when discussing identity fraud as it explains how an assassin could adopt the identity of a dead child to conceal his presence. When confronted with this information Mr Forsyth was surprised that no improvement in the security surrounding identity had been implemented. The aim of this investigation and the theft of these identities were to highlight the dangers of identity fraud.

In a report for the *Independent* newspaper by Judd (2005), figures on identity fraud which showed that one in four people have been a victim of this type of crime or know someone who has been are discussed. Included in this report is discussion of another example of simulated identity theft conducted by the magazine 'Which?':

> "The data published by the consumer magazine 'Which?' indicates that 10 per cent of people have been first hand victims and a further 15 per cent know someone who has had their identity stolen." (Judd .T, 2005: 16)

According to Judd's report, staff from 'Which?' magazine discussed how easily they were able to easily steal the identity of their editor Malcolm Coles:

> "'I couldn't believe how easy it was for someone else to assume my identity,' Mr Coles said. 'Sitting at my desk was a folder with my birth certificate, a print out of how often I went to the gym and my mortgage details.' 'If this is what an amateur can do, just imagine how easy it is for an experienced criminal.'" (Judd .T, 2005: 16)

For journalists, simulated identity theft is a means of highlighting the risks to the general public. Simulated identity theft also allows journalists to comment on the efforts of organisations to prevent and detect identity fraud. Aside from these attempts by journalists, simulated identity theft has also been used in America by investigators working for the Special Investigations office of the General Accounting Office (GAO). For three years, starting in 2002, a team of investigators from the GAO tested how counterfeit documents could be used to undermine various aspects of security in America. The areas of security the GAO tested by using fictitious and stolen identities were:

- Entering the United States
- Purchasing firearms
- Gaining access to government buildings and other facilities

- Obtaining genuine identification for both fictitious and stolen identities
- Obtaining social security numbers for fictitious identities

(Malfi .R.D, 2003: 1)

The GAO's investigation used simulated identity theft to test security and came to the following conclusions:

> "{1} government officials and others generally did not recognise that the documents we presented were counterfeit; {2} many government officials were not alert to the possibility of identity fraud and some failed to follow security procedures and {3} identity verification procedures are inadequate." (Malfi .R.D, 2003: 2-3)

Through the GAO's investigation, it was possible to highlight weaknesses both in terms of security procedures and in processes of identification. Both in journalistic investigations and the work of the GAO simulated identity theft has been used to gain insight into security surrounding identification processes. While simulated identity theft had proved useful in both journalistic investigations and the work of the GAO, it appeared that simulated identity theft has not been attempted in any academic studies of identity fraud.

Ethical, legal and practical considerations with an academic simulated identity theft

When it came to devising how simulated identity theft might be conducted, several ethical drawbacks were discovered. In previous examples of simulated identity theft conducted by journalists, the ethics of adopting someone else identity is rarely discussed. It became apparent, however, that in academic studies ethical guidelines would be central in any simulation of identity theft. Adhering to ethical guidelines established by the British Society of Criminology, and ensuring that no laws were broken during a simulation, raised questions about how to decriminalise any simulation attempt. In devising the simulated identity theft, it was determined that there would

always be a conflict between an ethical simulation and providing a realistic insight into identity theft. The more realistic the simulated identity theft is the more useful it could be as a means of estimating how actual instances of identity theft are committed. However the more realistic the simulation might be, the less ethical it would become. Issues of gaining consent, invasion of privacy and the legality of impersonation which had not been discussed during other simulations of identity theft are central to any plan to use simulated identity theft in an academic study. This aspect of the thought experiment also encouraged additional practical questions about how to establish a point of success in simulating identity theft and what methods of impersonation and surveillance would be appropriate.

At what point success?

One of the issues that had not been considered during the initial thoughts on simulated identity theft was how to determine when an adoption of another identity was successful. There are a variety of different methods of gathering and appropriating information about someone else's identity, but which ones are most significant in terms of proving identity? Also how many proofs of identity are needed to justifiably claim the theft of an identity? Is it enough to verbally claim you are someone else? Does duration of use influence the authenticity of someone's claim to an identity? One of the major changes the identity card scheme will introduce is the creation of a single universal form of identification. By doing this the scheme could bring an end to the current practice of confirming identity through requiring multiple paper proofs of identity.

How far could the simulation go?

The first goal of this study was to determine how identity fraud is committed now, prior to any introduction of an identity card. In previous attempts at simulated identity theft by journalists, the success of the simulation had been defined by the obtaining of documentation in someone else's name. By obtaining a driver's licence or birth certificate, it has been possible to illustrate the *potential* for abuse. Rarely were the simulations taken to the point of stealing other's people's money; often it was enough to establish the possibility of going forward to steal. In trying to examine the whole

process of how identity fraud is committed, in this study, it became apparent that obtaining only a paper proof of identity would not be enough. The simulation would have to go all the way from gathering information about the individual whose identity was being targeted, through to obtaining proof of identity and then obtaining resources (money, credit, items of value etc) under that name. By doing this, it was reasoned that not only would the process of detecting identity fraud by individuals and organisations be tested, but also this would enable a view of how effective current identity fraud prevention measures are. In terms of realism, the simulation had to include discussion and thought on the entire process of stealing someone's identity. This would mean that ethical and legal issues would be unavoidable. The next issue to address was determining how much of person's identity must be stolen.

At what point is an identity stolen?

In previous attempts at simulated identity theft, the goal had been to obtain paper proofs of identity such as drivers' licences; but is having a licence in someone else's name sufficient to declare that an identity has been stolen? Often in processes of identification a number of different documents are required as proof. In simulating identity theft it was reasoned that several forms of identification would be required, not only a driver's licence. In determining what proofs of identity would be required to show ownership of an identity, another issue was raised, namely that of who needed to be convinced by the impersonation.

Additionally, it was necessary to consider the issue of what forms of identification would produce the most accurate impersonation. Research into the identification process (see chapter 7) revealed that there were six key pieces of identification which were often relied on as proof of identity. These were:

- Birth certificate
- Drivers Licence
- Passport
- Bank or Credit Card account
- National Insurance Number
- Proof of residence (e.g. utility bill)

By obtaining these documents, it was thought that the researcher involved in the simulation would be able to obtain access to most of the things that a genuine identity holder would be entitled to. It was reasoned that by obtaining these forms of identification, additional forms of identification would become available to legitimate identity holders or identity thieves.

Discussing this issue, it was determined that while these documents are often used as proof of identity, it can be argued that they do not involve the theft of more personalised aspects of a person's identity. In addressing this issue, it became apparent that simulated identity theft might provide insight into how to steal a person's proof of identity but not a person's actual sense of self or personality.

Time taken to commit identity theft and the need for face-to-face interaction

Research into identity theft and fraud revealed that in some instances the actual time taken to impersonate someone could be very brief. For example, in an instance of online fraud such as phishing, a number of people can be targeted and have their details stolen and used in a short space of time (see chapter 7). At the other extreme in cases of wholesale assumption (see chapter 8) people can spend years trying to convince others of their impersonations (as in the case of Charles Stopford). This raised questions about how long a simulation of identity theft would take if it progressed to practical application. If the internet was utilised it could reasonably be assumed that very little time would be needed to instigate any impersonation of the research subject. This raised further questions over the need to use face-to-face interactions. An argument can be made that an identity thief will try to avoid detection wherever possible, and would therefore avoid unnecessary face-to-face meetings. An identity thief might also utilise technology which helps speed up the identity theft such as the internet (provided they have access). However, by avoiding the use of face-to-face interactions, the simulation would be limited in the forms of identification which could be sought, since several forms of identification provided by the state require a face-to-face meeting to confirm the applicant's identity. If face-to-face meetings were a required as part of the

simulation then this would have a knock on effect in terms of the potential research subjects whose identities could be used. The 'donor identities' would have to be ones that the researcher performing the simulation could reasonably be expected to impersonate.

Ethical considerations

As stated previously, the development of simulated identity theft was intended as a theoretical experiment into how a researcher might steal a person's identity. It was never intended as a practical experiment as the ethical implications for any research subjects were too great to ignore. However considering how a research subject might be treated and the effect the simulation might have on the research environment helped to clarify several issues.

In previous uses of simulated identity theft by others such as the GAO (2003) and Kenyon (2003), the issue of ethical treatment of research subjects had not been raised. However in this study the guidelines established by the British Society of Criminology (BSC) required that the issue of harm to research subjects be considered. In a simulation of identity theft, there are in effect two groups who could potentially be victimised. The first are individuals whose identity is being used (referred to as research subjects), and secondly there are the organisations who might be approached by the researcher.

The guidelines established by the BSC note that research subjects should not be harmed by the research. In effect, none of the research subjects in a simulation of identity theft should be harmed after the simulation was completed. In terms of realism and ethics, the choice of research subject would prove pivotal, as would the issue of how the research subject should be treated.

How are victims chosen in genuine cases of identity fraud?

The choice of a victim for simulated identity theft was difficult. In a genuine instance of identity theft, there is reason to believe that often identity thieves will use a piece of information they have happened upon, such as in cases where family members abuse

information on relatives. Or, in instances of identity theft by organised individuals, there is a process of trawling for information going out and searching for whatever is available. In either case, it is reasonable to assume that it is a law of averages as to whether or not the identity theft succeeds. Research by Bob Sullivan (2004) suggests that in instances of 'Phishing' there is a success rate of only 5%; however these types of gathering operations can be applied to millions of online users so if one person is chosen as a victim for the simulated identity theft there is no guarantee that it will succeed. In order for the simulated identity theft to work there would have to be several potential victims so that the success rate could be assessed.

Choosing a research subject or choosing a *victim?*

In simulated identity theft, the first element of the simulation would be the gathering and appropriation of information on the research subject. In the potential practical application of a simulation of identity theft, it would be necessary to investigate and gather information on the research subject. This would require, on the part of the research subject, a high degree of trust in the researcher in terms of how the information would be used. This proved a difficult issue to reconcile in the thinking on how the simulation might work, as access to the research subject's identity would also involve an invasion of their privacy.

One early idea for the simulation was to look at approaching family and friends as research subjects. It was thought that perhaps the pre-existing bond of trust would make the simulating of identity theft easier. The trustworthiness of the researcher would already be established and maintaining contact and a good relationship with the research subject would be easier. However upon further consideration the idea of enquiring into the personal lives of friends and family did raise questions over invading the privacy of people with whom there is a strong bond of trust and the potential strain this might have caused.

The alternative to using the identity of someone with whom there was a personal relationship was to the use the identity of a stranger or a volunteer. By using the identity

of someone with whom there was no or limited social interaction, it was reasoned, there would be less chance of jeopardizing or abusing a bond of trust. Thus the use of a randomly obtained identity was considered for a time. In this form of simulated identity theft, a research subject would not be chosen; rather several methods of gathering information would be used to 'trawl' for a vulnerable identity. One approach might be to conduct bin-raiding in residential areas and begin the simulation with any information which was discovered. In this simulation the victim would be chosen at random, depending entirely upon how vulnerable they were to impersonation. Once the research subject had been chosen, then their consent to proceed would have to be sought to proceed with the simulation.

Another approach considered was the use of a dead person's identity. This method has several distinct advantages. The use of a dead person's identity means, in terms of simulated identity theft, that the victim identity can be used in several ways without any need for negotiation with the victim as to what is permissible. Research on 'deceased' fraud by the Credit Industry Fraud Avoidance System (2008) revealed that there are two types of victim of deceased identity theft relating to either those who have recently died or to the identities of dead children. The use of a recently deceased person's identity involves obtaining and maintaining the identification the deceased had during life. The alternative is the use of birth certificates of dead children who were born at around the same time as the person committing the simulated identity theft, so as to ensure a match with regard to age of the victim. Using the birth certificate of a dead person means that there will be very little additional identification past the birth certificate and the possibility of detection is minimal. The use of a deceased person's identity is discussed further in chapter 8.

Ethically, the use of the identities of the recently deceased or a dead child raises a number of moral issues. Obtaining consent would involve speaking to relatives of the deceased; in either instance it was assumed that consent would be difficult to obtain. While the actions taken during the simulated identity theft would focus on obtaining paper proofs of identity, the concern would be that relatives of the deceased would see

these actions as commandeering the identity or as an abuse. While identity in the simulation was viewed as more of an issue of proof used in the identification process, for many an identity is a representation of self, and using the identity of a dead person, it can be argued, would involve adopting their sense of self. The effect this could have on people's perception of the deceased could be damaging. In the case of Charles Stopford it was reported that his impersonation of Christopher Buckingham caused Buckingham's mother Audrey Wing a great deal of distress. In the documentary *The Real Jackal* (2006) Wing was interviewed about the discovery that someone had been impersonating her dead son. Her initial response upon hearing that someone called Christopher Buckingham was alive was an assumption that her son was still alive, despite his death as a baby. The discovery of Stopford's use of the identity also raised old memories of the death of her son for Audrey Wing. In the documentary, it is clear that remembering the death of Christopher Buckingham causes Audrey Wing a great deal of distress.

While it is not technically illegal to use another person's birth certificate (unless it is as a part of a wider criminal conspiracy) ethically is it right or fair to use a dead person's name? Should consent be gained from their family and how much use should be made of this document and in what respects should it be used? These issues raised questions about the wider influence of a person's identity. It can be argued that any impersonation will not only affect not only the genuine owner of the identity but also those associated with that person. In cases of identity fraud where criminals seek to avoid prosecution, the effect has often been to victimise not only the individual whose identity was stolen, but also people who interact with that identity. Examples of this can be seen in chapter 8.

The final approach considered was requesting volunteers to take part in the simulation. This approach would involve simulating identity theft on people with whom there was no personal relationship. This approach would seem most appropriate as it would allow people to choose whether or not to participate. But this approach also raises questions about how informed the research subjects should be of what would happen to them. The B.S.C. guidelines state that research subjects should not be harmed by taking part in the

research; this meant that anyone taking part in the simulation would have to be protected in some way from the actions of the researcher simulating the identity theft. In order for any practical application of the simulation to be an accurate analysis of how identity theft is committed, there would have to be some form of resource taken from the research subject. Also, the research subject would have to be unaware of what was happening so the ability of the research subject to detect the identity theft could be assessed.

However to keep the research subject safe from the financial and possible emotional damage of being a victim of identity theft, they would have to be informed of what was happening and their consent would be needed. If the research subject were aware of what was going on then there would be the potential for them to interfere in the process of gathering information on themselves. The research subject's efforts to secure their identity might change because of the simulation. This could provide an inaccurate view of the research subject's ability to detect and prevent identity fraud. It was also determined during this stage of the simulation that research subjects might request that certain areas of their personal life were not investigated. It was determined that there would be a potential for the research subject to censor or limit the scope of the information gathering elements of the simulation in order to maintain a degree of personal privacy. This resulted in a conflict between keeping the simulation realistic and keeping it ethical if it ever progressed to practical application and this conflict could not be resolved.

Similar considerations obtain with regard to the organisations it would have been necessary to approach in the later stages of practically application of the simulation. If organisations such as the DVLA or any financial institutions had been informed and involved, it is reasonable to assume that they would either oppose their inclusion in the simulated identity theft or would have tried to ensure the failure of the experiment. In order for the simulated identity theft to be a representation of what might happen in a genuine incident of identity theft, the victims (both the individual whose identity has been stolen and the organisations targeted) must be unaware.

Previous attempts at simulated identity theft by Kenyon (2003) and Aaron (2007) had, in a way avoided this issue of research subject awareness by choosing people they would not feel uncomfortable about victimising. In the case of Kenyon, he targeted David Blunkett, the then Home Secretary, and a major advocate of the identity card scheme. Arguably, by targeting a high profile person, the actions of Kenyon rather than appearing as a crime or unethical, were seen as a demonstration or a stunt to illustrate a point. Also, the simulated identity theft used by journalists from 'Which' magazine was used to further the success of the magazine as a whole. No evidence could be found to suggest that either Kenyon or the journalists at 'Which' faced any legal action over their actions. This may be because, as journalists their actions were not perceived as malicious or an attempt to defraud anyone; it might also be that given the way they adopted the identities of others, there was no perception of harm on the part of their victims. In both accounts, people's personal information had been used without their consent, but both Kenyon and the journalists at 'Which' had not abused the identities they had access to. An important distinction can be made here between impersonating someone and misrepresenting their identity (this distinction is discussed in more detail in chapter 8). This does not excuse the unethical accessing of another person's identity, but it does show how there can be a certain ambiguity around efforts to impersonate someone for reasons other than financial gain.

Should research subjects be informed?

The issue of whether or not the research subject should be aware of the simulation is the major obstacle to the practical application of this thought experiment. In many respects, at this stage, it became apparent that identity fraud could not be simulated accurately without the research subject being victimised to some degree. It became apparent that the standards of practice in an academic study were different to the standards applied to journalistic investigations and the work of the GAO. The abuse of a person's identity cannot be justified on the grounds of research alone. By planning out how to treat research subjects, the value of personal privacy became apparent.

Invasion of privacy

During the development of the simulation, it became apparent that the line is very thin between information intended to gain access to social institutions and information of a personal and private nature. This is intentional, as the idea behind various security measures using identification is that the information used such as mother's maiden name is not something people will openly share although this is not to say this information is not obtainable from other sources. So any attempt to instigate a practical simulation of identity theft would entail learning a variety of personal facts about the research subject. In the debate over identity cards, the argument is often used that 'if you have nothing to hide you have nothing to worry about'. This phrase is used as justification for identity cards, but for individuals there is the power (some would argue the right) to include and exclude other people from knowing certain things about themselves. In the process of stealing an identity, a person's ability to place boundaries on what the identity thief learns is gone.

When developing the simulation of identity theft it was determined that it should be a thought experiment which tests different methods of gathering information about people. This could involve methods of gathering information from both documentation going to and leaving the research subject, and also from direct observation of the research subject. All of the forms of gathering information considered involved some degree an invasion of privacy. For example, by reading a person's private mail or email, it is possible to obtain pieces of information about their identity which can be used in the simulation of identity theft but at the same time personal correspondence includes information that research subjects may want to keep private. Often the information which is used to enable the impersonation of someone is the same as the information people may want to keep private for personal reasons. While the issue of privacy is something which may result in research subjects refusing to participate, it is also worth noting that people can be quite open with their personal details.

Willingness to share information

Ironically, while this study is based on a perceived increase in concern over the identification process, often the details that we hold so personal to our sense of self are the ones we give freely when asked. One of the methods of committing identity theft is by simply asking your victim for these personal details. In the terminology of identity theft, this is known as pre-texting or social engineering (see chapter 7). Individuals divulge private information about themselves, because, arguably, divulging these details is a daily occurrence and part of a normal social life. As a matter of course, we identify ourselves and use various identification processes. Awareness of the risks of identity theft has still to be fully developed so while there is awareness of the danger of leaving identifying documents out for people to take, the risks posed by simply asking are still underdeveloped. In a discussion of this issue with a fraud investigator at a conference for the Department for Works and Pensions (2005) it was explained how during a discussion with a taxi driver the investigator had been able to elicit enough information from the driver to put his identity at risk. It was not until the end of the journey that the investigator revealed just how much had been gathered from the driver without his being aware of it.

Legal considerations and protecting the researcher

As well as concerns about how to treat the research subject during the simulation of identity theft, there are also concerns with regard to the potential risk faced by the researcher simulating identity theft. Legally it is not a criminal act to claim you are someone else; it is only when someone tries to validate their claims, through a social institution that is required to validate or confirm an identity for legal reasons, that it becomes criminal and / or fraudulent. Simply declaring oneself to be someone else is not enough to commit identity fraud; there must also be an attempt to validate that claim.

In addition to the introduction of an identity card the National Identity Card Act 2006 also introduces laws against false representation. False representation means that pretending you are someone you are not, or collecting information to assume another identity, becomes a criminal act as soon as it is used with another person who is

unaware of your true identity. False representation requires that the person who is being presented with the false identity is in some way deceived or unaware of the deception.

In a practical simulation of identity theft, the use of deception is something which would place the researcher at risk. In order to avoid false representation it would be necessary to inform people that the identity being used is not the researcher's true identity. However, this would undermine one of the goals of simulating identity theft, namely determining how easy it is to deceive people and for that deception to be detected. It can be argued that this situation places the researcher in a 'catch 22' situation: if they want to simulate identity theft they must use false representations; but if false representation is used then the researcher is at risk of criminal prosecution.

The research environment

The final ethical issue which was considered was the research environment and how simulating identity theft could affect future efforts to research identity fraud and identity cards. Future involvement with organisations such as the banking and credit industry, the DVLA and other providers of identification might be difficult to maintain if the simulation had gone forward. In previous attempts at simulating identity theft the goal has been to highlight deficiencies and failures in protecting the identification process. When in 2003 Paul Kenyon simulated the theft of David Blunkett's identity, his aim was to show how current levels of security were inadequate. Equally, the efforts of the GAO investigators in 2003 were designed to highlight any problems in security. If this simulation had gone forward it is reasonable to assume that some organisations might have taken issue with being deceived. While the ability to detect and prevent identity fraud is something the simulation could analyze, it is also important to maintain good relations with organisations involved in the identification process in order to enable future research.

Criteria for the simulation

In order to determine the limits and scope of the simulation a series of goals were developed to inform the later stage of constructing a guide to simulating the theft of an identity. These goals were:

- To establish the whole process of how to steal someone's identity from beginning to end
- To assess the ability of social institutions to detect identity fraud
- To assess the ability of individuals to prevent identity fraud
- To assess the ability of social institutions to prevent identity fraud

How to simulate identity theft

When developing simulated identity theft it was necessary to do significant research into various cases of identity theft and fraud. Cases from the U.K. and U.S.A. were studied to determine what techniques are used to gather information on people, and how that information can be used to impersonate another person.

When thinking about how to simulate identity theft, it was important to determine what the end goal of the simulation could be. Also, could a fictitious identity be used instead of another person's identity? Most of the thinking on simulated identity theft had been done in the context of stealing another person's identity. But an equally viable approach might be the use of a fabricated identity where no 'donor identity' would be needed.

Fictitious identities in simulated identity theft

While the use of a fictitious identity had not been considered, upon further consideration it became clear that the process of generating one would not be difficult. With the advent of personal computers, scanners and printers it would be possible to fabricate copies of official documents. By taking an official document, for example an official document from Bangor University, it is possible to scan the document into a computer, cut and paste out the text so that the document appears as a blank apart from the header and then fill in new information, print the new document and use it. With computers and

printers so prevalent in society, it is not uncommon for documents to be printed copies. In many instances, documents or forms are available online and are intended to be downloaded and printed. The drawback of fictitious documents is that they do not exist in departmental databases or official records. Also in some instances, such as passports, a great deal of effort has gone into making them unrepeatable by private citizens, through the use of UV ink, special papers and document checks at point of use.

A fictitious identity would require a great deal of pretexting and social engineering to establish and conceivably there would be areas of society that would be closed off to it such as passport control. The drawbacks of using a fictitious identity were also considered. These drawbacks were predominantly associated with not being able to consider the impact that identity theft has on its victims.

Simulated identity theft

Presented below is a discussion of how the simulation could have been conducted; while none of these actions were actually carried out the planning of them proved useful in conceptualising how identity theft might be committed.

This simulation represents a form of identity theft which seeks to break as few laws as possible; so for example the initial information on a 'donor identity' would be obtained legally from social institutions rather than the individual. By doing this it was thought that the simulation could show how vulnerable people are to others appropriating their information and impersonating them. This simulation also represents a concerted effort to steal one specific person's identity.

The process of targeting one person's identity specifically would be used by someone who planned a prolonged period of use with that identity. An example of this would be wholesale or partial assumer's efforts to swap identities and take up their victim's name (see chapter 8 for details on wholesale and partial assumers). Here the first step is to choose a victim and then locate their information; an alternative approach would be to begin with a location or piece of information and then build on that. This alternative

happens when bin raiding is successful in finding a valuable piece of information or if someone's mail (both real and virtual) is stolen.

One way this simulation of identity theft differs from identity theft used for financial gain is that it would require the spending of money to establish the researcher simulating identity theft as the legitimate identity holder. In many instances of identity theft it is left to the victim to notice that identity theft has occurred. This is because it is not until the victim sees that their identity is being abused that the crime is detected. Only in specific instances is identity theft noticed by social institutions such as in the case of Charles Stopford's impersonation of Christopher Buckingham where a cross reference of death certificates and passports detected his impersonation. As a general rule however if the victim does not notice the impersonation no one will detect the impersonation as long as there is sufficient information on the part of the impersonator.

Step 1 Birth Certificate

The practical stage of simulating identity theft would have to begin with legally obtaining the research subject's Birth Certificate. A copy of this can be obtained from the registry of Birth, Deaths and Marriages. With the copy of the research subject's birth certificate, other information can be gathered: parents' names and the victim's date of birth and location of birth. With the names of the parents, a search of the registry of marriages can be done to find the marriage certificate of the research subject's parents, and this can lead to the research subject's mother's maiden name (sometimes used as a question in security checks). Also, by estimating the age of the research subject and their parents, it is possible to go to the Friends Reunited website and attempt to find out what schools the research subject and their parents attended (which is sometimes used as a security question). With the birth certificate, the research subject's date of birth is revealed so that the research subject's age today can be known. Ideally, the research subject should be close to the age of the person assuming their identity, in case there is a need to impersonate them in a face-to-face interaction.

Step 2 Geographic location

With the name of the research subject, the next step would be to attempt to locate their home. The home is a vital component as it acts as store house for information intended for and leaving the research subject. As an identity thief, the goal is either to take information from people through direct theft (a method not used in this study), or to intercept information intended for the victim. Information discarded by victims can also be used to steal an identity.

In order to find the research subject's home by legal means, it would be necessary to first check the phone book to see if they are listed and/or check the electoral register at the local library for the victim's location. Recently concern over access to the publicly available electoral register for this purpose has lead to the option of having your details kept off it. If the home address of the research subject can be found, a process of intercepting information intended for the research subjects, or information discarded by the research subject, can begin. Mail can be taken from the research subject's post boxes (if they have one) outside the house, or a request for mail redirection can be made to the Royal Mail. As well as taking real mail, there are various methods of obtaining emails. Key loggers are devices that can be attached to computers to monitor what keys are typed on the key board (providing access to Personal Identification Numbers and answers to security questions); this would require access to the interior of the house. One way to gain access to the interior of the house would be to break into the house or to use deception to elicit entry; both methods were deemed unacceptable for legal and ethical reasons. Alternatively, spyware computer programs can be downloaded in emails on to a person's computer, providing access to the information stored there.

As well as intercepting information before it reaches the research subject, or from the research subject's computer; bin-raiding will provide access to information discarded by the research subject. Among the various types of information available from bin raiding are bank statements, credit card information, old or out dated forms of identification (cut up debit or credit cards), and also there is general evidence of the type of lifestyle the research subject is living. Bills and receipts from shops might show how much money

they are likely to spend and where. Trying to intercept information before and after it has reached the research subject is in some ways like gold prospecting: there is no guarantee that anything useful will be found but there is a chance that something highly valuable will be discovered.

If information was gained from bin-raiding or redirecting mail, then it would enable the takeover of accounts that the research subject has opened (see chapter 6 for account takeover). If however information on presently open accounts is not forthcoming then it may still be possible to use the information gained to open new accounts that the research subject is not aware of, in the research subject's name. In order to do this, the research subject must be separated from their identity so that any further activity planned in this study would not be noticed by the research subject.

Step 3 Setting up an alternative repository for documentation

With a degree of information derived from the birth certificate and from monitoring information going to and coming from the research subject, the next step is to purchase a post office box for any correspondence obtained while using the research subject's identity. When setting up bank accounts, or accessing forms of identification there must be a geographical point for this information to be sent to.

An alternative to a post office box is to secure a flat or house in the research subject's name, so that bills for electricity and other amenities can be obtained. Additionally, as well as creating a geographical location for all the correspondence attracted while using the research subject's identity, it will also be necessary to obtain a mobile phone in the research subject's name.

By obtaining a different residence and phone line the identity thief can apply for different forms of identification and set up bank accounts without having to use the genuine identity holder's address or phone number. In effect, the identity thief establishes a parallel existence for the identity. There is the genuine identity holder and their contact details and residence, and then parallel to this there is the identity thief with

a separate set of contact details and residence. This reduces the likelihood of an organisation involved with the identity thief contacting or interacting with the genuine identity holder and thereby exposing the activities of the identity thief.

Step 4 Additional evidence

Aside from having the appearance of a residence and a means for people to contact the individual simulating identity theft instead of the genuine identity holder it is also necessary to create the impression that the researcher simulating identity theft has lived as this research subject. This will require obtaining additional forms of identification such as a driver's licence or evidence that other social institutions have trusted the identity thief in their use of the research subject's identity.

The obtaining of this evidence may be in some instances quite easy as there are several forms of identification which have minimal security checks. This is because there is no direct financial benefit to their theft. Memberships in social groups for instance or gaining qualifications either professional or academic are examples of this. There are several academic qualifications which can be bought from the internet from fake or counterfeit universities. Aside from forged qualifications, there is also qualification from distance learning courses where their identification checks can be manipulated. It is even possible to buy a peerage from websites such as nobility.co.uk, allowing the identity thief to raise the social status of the stolen identity. In obtaining additional forms of identification, people begin to trust that the identity thief is the genuine holder of the identity even though they are not.

This process will involve spending money; however, this merely reinforces the idea that the researcher conducting the simulation is the genuine identity holder. The goal here is to establish several bonds of trust within society under the research subject's name; the more bonds created the more proof exists that the identity thief is the genuine identity holder. This is important, as providing background information that the identity thief can control will allow for interaction with organisations which require some form of background checks.

Step 5 Approaching financial institutions

By taking these steps, it is possible to give the impression to social institutions such as banks and credit companies that they are dealing with the genuine identity holder. According to Sullivan (2004) one of the problems facing the credit industry is that it is too eager to set up accounts and then deal with any problems it faces with identity theft when genuine identity holders discover there is a problem. With the advent of the internet it has become possible to set up bank accounts over the internet thereby limiting the amount of face-to-face interaction and allowing for multiple applications to numerous banks or credit agencies in a short period of time.

Step 6 Achieving an all-round impersonation

If steps 1-5 are successful, then it is conceivable that the researcher conducting the simulation could live under the identity assumed. There would be an address, phone number, bank account, and state documentation all under the researcher's control. The only area where the simulated identity thief would face difficulty in maintaining the identity is when trying to obtain the National Insurance number of the research subject. Without this number, the only places the researcher could work would be in jobs that are 'cash in hand'. These types of jobs form the 'black economy' (discussed in chapter 3) which attracts people who wish to avoid paying tax or involvement with government work, for instance illegal immigrants. This may be beneficial for it would mean the researcher would not have to pay taxes. However this would limit the researcher to relatively low income work which would have none of the security found in legitimate work. If the researcher wanted a job that involved a pay check it would involve the obtaining of the research subject's National Insurance number. This would also improve the chances of obtaining a passport by making an application in the name of the research subject.

There are ways of obtaining someone's National Insurance Number such as theft from the home or theft of employment records. But in simulating identity theft these avenues would be closed off for ethical reasons. The method this study imagined using would be pretexting with the research subject. The researcher simulating identity theft would use

the information already gathered on the research subject and contact them or someone they are involved with. This would involve pretending to be an organisation such as the Department for Works and Pensions that the research subject would expect to know their National Insurance number. The key to the pretexting is to imply that rather than trying to find out something the identity thief does not know we are in fact re checking information already known. While people will be cautious about revealing information it can be argued that if instead they believe they are confirming something already known they will not feel as though they have anything to protect. This pretexting would be done via phone or over the internet. Neither of these approaches are guaranteed to be successful as scams involving pre-texting over phone lines and the internet have been publicised in the media for instance Phishing emails (see chapter 7 for examples of phishing emails).

If successful in obtaining the National Insurance number then it would be possible for the researcher to attempt to obtain a passport. Obtaining a passport would be important when it came to reinforcing the researcher's claim to the identity. After obtaining a passport the next step would be to try and obtain a National Identity Card (if the scheme were operational at that time).

Another approach that could be used with the passport is to move to another country and use the stolen identity there. The use of travel to other countries is a useful approach as it can obscure the initial identity theft. It can be argued that this is something Charles Stopford did when he stole the identity of Christopher Buckingham. By moving to another country, the identity thief would be using the identification documents with a new administrative system that would have to work a lot harder to detect the identity theft.

This process would take time and require a great deal of research into the life of the research subject; it would also require a great deal of effort and financing to establish the separate address and forms of identification. In a genuine case of identity theft, it can be argued that the criminals would not focus on the victim, rather they would be more

focused on the information, credit card numbers, National Insurance numbers etc., and any paper proofs of identity the criminals found would be exploited to see what could be gained from them rather than to focus on the identity. In a way, the goal of identity theft for profit is not to obtain the identity but what the identity provides. The model of identity theft represented in this simulation of identity theft is a partial assumption of identity. Here the goal is not simply to dispose of the identity once financial gain has been made.

Why this approach cannot be used in researching identity theft

As stated earlier the simulation presented above was always intended as a thought experiment. This was due mainly to the ethical and legal drawbacks of attempting to enact it and as such none of the actions discussed were attempted. However, in 2007, a television documentary for Channel 4 by Bennett Aaron on identity theft did use actions which could be considered as a practical example of simulated identity theft. During this documentary, Aaron tried to illustrate the dangers of identity theft; however in his efforts to show how dangerous and damaging identity theft is, he openly abused the identities of others.

Aaron was himself a victim of identity theft and was hoping that by using identity theft in his documentary he could highlight the dangers of this crime. During the making of the documentary, Aaron raided a man's bins, and used information gained there to purchase items in his name. After achieving this instance of identity theft Aaron went to the house of the man whose identity he had stolen and showed him how he had stolen the identity and the items he had purchased.

While this was a powerful illustration of the danger of identity theft, it failed to acknowledge the abuse Aaron himself had done to the victim's identity. The man whose detail had been taken showed no sign of consenting to the theft of his information. While he agreed to take part in the documentary, it was evident that he was unaware of what had been done to him until presented with the findings of Aaron's bin-raiding.

In another example from the documentary, Aaron also obtained a driver's licence in the name of Charles Clarke (the then Home Secretary) to show how anyone is at risk. After trying and failing to arrange to meet Charles Clarke, Aaron went to London with a poster size copy of the drivers licence and displayed it in front of the Houses of Parliament. At the end of the documentary, it was revealed that Aaron had been arrested and cautioned for his activities.

This documentary helped to illustrate the dangers of identity theft to the general public, but for this study it has also helped to show the dangers of simulating identity theft. Aaron began the documentary by noting how he felt when his identity was stolen, but in the rest of the documentary he happily stole the identities of others without considering what he was doing to them. Stealing an identity to show the danger and abuse that can happen when an identity is stolen seems an unethical approach that undermines the message that identity theft is a personal abuse. While there is no practical example of simulated identity theft as described, in this study, we can look to the actions of Aaron as an example of the kinds of ethical and legal implications that prevent academic studies of identity theft from using simulated identity theft.

Inaccuracy simulating modern identity theft

According to Frank Abagnale (2007) there has been a shift in the nature of identity theft. Where conmen in the 1960s had to focus more on the victims and what could be gained from them, the modern day identity thief focuses on the information he/she can obtain. Abagnale compares the activities of modern identity thieves to workers on a production line processing the identities they have stolen in an industrial sense *en masse*.

In this respect, simulated identity theft is not in keeping with the perceived normal processes of modern day identity thieves. In considering how to simulate identity theft, there had to be a focus on the research subject (the victim) in order to avoid unethical treatment by the researcher. The simulation also had to demonstrate how susceptible different types of identification are to identity theft and identity fraud.

This is not the motivation for organised crime groups seeking to make money from credit scams, or people-smuggling operations in the U.K. Simulated identity theft, while showing the process of stealing certain parts of a person's identity, does not represent the true manner in which criminals adopt or impersonate the victim. In the simulation, the identity of the victim is developed and constructed, whereas in a more conventional case of identity theft the identity is abused.

Researching the national identity card scheme

Aside from researching the various methods of committing identity theft, it was also necessary to monitor developments with regard to the proposals for the National Identity Card Scheme. This can at times be difficult as the proposal for the ID card scheme have been subject to various changes since 2002.

This has made the task of assessing what effect the identity card might have on identity theft and identity fraud harder, as the exact nature of the proposed scheme is still in flux. It can be argued that the use of identity cards will always be open to alteration by public protest and political disagreement, with regard to the aims and objectives of the scheme. In order to adapt and include these variations it also important to keep track of political debate concerning the identity card, the popularity of the scheme and the discovery of security issues.

Researching a new area of study

Researching the national identity card scheme at this stage of its development has its difficulties because the scheme is still being amended and changed. Looking at the operation of identity card schemes in other countries and the political discourse for and against identity cards can provide some insight into how identity cards might work in the U.K. However given that the scheme is still under development this study can only provide an informed snapshot of what is happening with the scheme up to 2009.

One way to gain an insight into what impact an identity card scheme might have is to look at identity card schemes operating in other countries. According to Privacy

International (1996) there are numerous countries worldwide that use an identity card scheme:

> "Around a hundred countries have official, compulsory, national IDs that are used for a variety of purposes. Many developed countries, however, do not have such a card. Amongst these are the United States, Canada, New Zealand, Australia, Ireland, the Nordic countries and Sweden. Those that do have such a card include Germany, France, Belgium, Greece, Luxembourg, Portugal and Spain.
>
> The use of sectoral (specific purpose) cards for health or social security is widespread, and most countries that do not have a national universal card, have a health or social security card (in Australia, the Medicare Card, in the United States, the Social Security number), or traditional paper documents of identity. The reverse is also true. In Sweden, while there exists a ubiquitous national number, there is no single official identity card.
>
> Generally speaking, particularly in advanced societies, the key element of the card is its number. The number is used as an administrative mechanism for a variety of purposes. In many countries the number is used as a general reference to link the card holders activities in many areas." (Privacy International, 1996: 2)

By looking at European identity card schemes it maybe possible to learn about how the identity card scheme in the U.K might be administered and run. The process of applying for an identity card and how the identity card is used on a day to day basis by citizens in countries such as Belgium, France and Portugal could provide some insight into how citizens in the U.K. will engage with the scheme. It might also provide some insight into the benefits the scheme might provide with regard to the administration of health care provisions, state benefit and the general process of identification people are involved in on a daily basis. As discussed in chapter 4 identity cards are not a new idea. Although there are things we can learn from looking at other identity card schemes; there are

aspects of the new U.K identity card scheme which distinguish it from other schemes established identity card schemes.

Firstly the new U.K identity card scheme will not be a paper based identity card it is a smart electronic identity card. Established European identity card schemes often employ a paper based identity card which is a simply a paper or plastic card linked to a central register. Smart electronic identity cards according to Lyon (2004) include an embedded computer chip which holds information such as biometric data. In effect the identity card holds its own information and is not just a document that links to a centralised register of information. This new approach to identity cards is being developed in several countries most notably in South East Asia. Lyon (2004) notes that China, Hong Kong, Thailand, Malaysia and Singapore are all investing in smart electronic identity cards with Austria, Belgium, Germany, Russia and Spain considering the introduction of new identity card schemes. The technology that these particular schemes rely on varies and could influence the effectiveness of the various schemes. How each smart electronic identity card scheme operates and the manner in which the schemes operate and counter identity related crime will vary. So while there is some benefit to looking at pre-established identity card schemes it is important to recognise that the U.K scheme is part of a new wave of identity card schemes which are being established.

Also the U.K scheme is a new form of identification, not since the 1950s has the U.K operated an identity card scheme. How the new identity card scheme will be received and adopted by people in the U.K to a degree cannot be determined by looking at countries which have a pre-existing identity card schemes. The U.K scheme is being introduced at a time when a concern over identity security is a major concern for both the government and the general public. In many respects the nature of the scheme reflects these concerns with an emphasis on biometric security, and the role the identity card can play in preventing identity fraud, terrorism and illegal immigration. Identity card schemes in Europe emphasize improvements in health and welfare provisions, and are ultimately a tool of administration and not security. This is not to say they do not play some part in crime prevention or detection. But in comparison with the U.K.

scheme which has placed biometric security at the forefront of the scheme, European identity cards do not involve the same (proposed) levels of scrutiny holders of a U.K. identity card will be under.

The issue of security and crime prevention associated with the U.K scheme bring into play issues of civil liberty and the limits of state surveillance. These developments are important to consider in their own right as they show how concerns over data security, trust in the government, biometrics, cost and civil liberties have dictated the development of the scheme. The recent credit crunch in the U.K. is also a factor which may influence the future of the identity card scheme. Critics of the identity card scheme such as Privacy International, NO2ID and Defy ID have often pointed to the rising cost of the scheme as a reason to discontinue plans to introduce identity cards. How the scheme will survive through these times of economic difficulty is debateable. It may be that in order to counteract concerns over cost the identity card scheme is curtailed or amended to make it cheaper. This may in turn result in the scheme being less effective as a means of preventing crime or detecting it.

Despite concerns over the credit crunch in May 2009 the Identity and Passport Service began a pilot of the voluntary identity card scheme in Manchester indicating an intention to go ahead with the scheme. It has also been noted by Woodhouse (2009) that the government has introduced a 'poison pill' strategy which will result in a £40 million fee to companies involved in introducing the Identity Card scheme if the scheme is discontinued. This fee would make the plans of the Conservative and Liberal Democratic parties to discontinue the identity card scheme costly.

Researching political developments around the identity card

The politics surrounding the identity card scheme have raised several questions about the future of the identity card. As discussed in chapter 4 both the Conservative and Liberal Democrat Parties have made discontinuing the identity card scheme a part of their policy commitments. According to Conservative shadow Home Secretary Chris Grayling:

"I see little reason why the rules to a national identity register such as that proposed by the government at a time when the nation's finances are straitened and when genuine questions arise about civil liberties seem to suggest that it is a project that we do not need to pursue." (Grayling .C, 2009: 1)

The Conservative party aside from denouncing the identity card scheme have also sent letters to companies taking part in the identity card scheme outlining their intention to discontinue the scheme. Leader of the Liberal Democrats Nick Clegg has vowed to face court proceedings rather than register for an ID card if the government presses ahead with plans to make them compulsory. The Liberal Democrat shadow Home Secretary Chris Huhne has also criticised the identity card scheme stating:

> "These expensive and intrusive plans should be ditched now. The vast amount of money would be far better spent on something that will actually fight crime and terrorism – ten thousand more police on the street." (Huhne .C, cited in Tall .S, 2009: 1)

Perhaps one of the most damaging criticisms of the identity card scheme came from David Blunkett in 2009. At the InfoSec security conference 2009 Blunkett argued that the identity card scheme should be scrapped in favour of the mandatory biometric passport system. The former Home Secretary argued that the biometric passport would not only be a cheaper alternative, but would also alleviate the general public's fears over National Identity Register.

> "People don't worry about the Passport Agency but they do worry about some mythical identity database," (Guardian.co.uk, 2009: 2)

The criticisms posed by David Blunkett have been highlighted by both the Conservative party and the Liberal Democrats as a sign that the scheme should be discontinued.

Liberal Democrat shadow Home Secretary Chris Huhne responded to Blunketts comments by saying:

> "When even the father of ID cards spurns them, the idea is truly an abandoned orphan." (Huhne.C, cited in Liberal Democrats website, 2009: 1)

These objections have placed a definite question mark over the long term survival of the identity card scheme. Aside from the issue of whether or not the identity card would survive a change in government the politics surrounding the identity card scheme has also been influenced by the public perception of the government and its scheme. Concern over both civil liberty implications of the identity card and the trustworthiness of the government to operate the scheme has influenced the debate.

The view that identity cards are part of an effort to create (or perpetuate) a 'surveillance society' has led to a great deal of opposition from protest groups and civil liberty advocates such as Privacy International, Defy ID and NO2ID. The effect opposition to the identity card scheme from the general public might have on the continued popularity of the scheme is debateable.

Often arguments over the identity card scheme involve referral to public opinion polls, with both supporters of the identity card scheme and opposition groups reinforcing their view of the identity card with referral to polling data. Surveys commissioned by the anti-ID card group NO2ID between 2005 and 2007 have routinely posed the same question:

> "Q.1 The Government has proposed the introduction of identity cards that, in combination with your passport, will cost around £93. From what you have seen or heard do you think that this proposal is a...?" (NO2ID/ICM, 2007: 2)

The 2005 survey found that 50% of people thought it was a good idea (14% very good, 36% good) and 48% thought it was a bad idea (23% very bad, 24% bad) with 2% refusing to answer or not knowing. In 2006 the survey found that 52% of people thought it was a good idea (16% very good, 36% good) and 45% thought it was a bad idea (20% very bad, 26% bad) with 2% refusing to answer or not knowing. The 2007 survey found that 54% of people thought it was a good idea (14% very good, 40% good) and 42% thought it was a bad idea (17% very bad, 25% bad) with 4% refusing to answer or not knowing. This implies that feelings on the identity card are still mixed as to the whether or not the scheme is a good idea. What effect combining discussion of how people feel about the identity card with the issue of cost has on people's view of the scheme is debateable it may influence their response to the question. Equally it can be argued that discussing the identity card with regard to terrorism, civil liberties and privacy might also influence people responses. Despite these possible biases, these surveys suggest that there is some shift towards finding the scheme more acceptable; but how these numbers will be affected if and when the identity card scheme becomes compulsory is debateable. (see appendix 7 for NO2ID.ICM Polls)

An assessment of awareness and demand for the Identity Cards Scheme in 2005 by the Home Office also looked at the popularity of the identity card scheme. In this survey 983 people aged 16-75 were sampled with an additional sample of 126 parents of children aged 15 years old. This was done as part of quota sampling to ensure representation of subgroups. The survey sought to provide a representative view of the U.K. population with regard to gender, presence of children, working status and no passport ownership. This survey found that 73% of citizens support the proposed identity card scheme.

According to the UK Polling Report (2009) surveys on the popularity of ID cards commissioned for the Home Office, NO2ID and various newspapers, also report mixed response to the popularity of the identity card scheme between 2004 and 2009. With finding like this, it can be argued that the acceptance of the identity card scheme by the general public is still debateable. How people's feelings over the scheme will change

when they are required to have an identity card and must pay for it is debateable. The degree to which people must use their identity card and the convenience/inconvenience of having the identity card will affect the popularity of the scheme. How much the identity card will cost the individual citizen may also influence the appeal of the scheme.

The prominence of the identity card in preventing or detecting terrorists, illegal immigrants and identity thieves will also play a role in the popularity of the scheme (see chapter 9 for details). As the scheme has not won the overwhelming support of the general public it is more important that the government appear competent and trustworthy, so as to ensure that when the scheme does come into effect support does not fall away completely.

However since the ID card scheme was first proposed in 2002 by then home secretary David Blunkett, there have been four changes in home secretaries Charles Clarke, John Reid and Jacqui Smith and as of May 2009 Alan Johnson. Clarke and Reid were both been forced to resign due to failure to maintain accurate records of criminals. Aside from these controversies there have also been several incidents of confidential and private data being lost by the government (see chapter 9 for more). A major part of the new identity card scheme is the creation of a National Identity Register a database of personal information. Criticism of the government's ability to ensure the safety of information in pre-existing databases raises doubts over their ability to secure and protect data in the National Identity Register. The government's ability to effectively introduce new information technology projects has been criticised both in terms of human rights implications and the effectiveness of schemes. The Joseph Rowntree Reform Trust (2009) conducted a review of 46 government databases and assessed them in terms of their adherence to human rights and data protection legislation. The report – *Database State* (2009) uses a traffic light system with databases where there were no problems being referred to as green, databases with moderate problems referred to as amber and highly problematic systems were red. According to the report:

"Of the 46 databases assessed in this report only six are given the green light. That is, only six are found to have a proper legal basis for any privacy intrusions and are proportionate and necessary in a democratic society. Nearly twice as many are almost certainly illegal under human rights or data protection law and should be scrapped or substantially redesigned, while the remaining 29 databases have significant problems and should be subject to an independent review."

(Anderson .R et al, 2009: 2)

In the review one of the databases looked at was the National Identity Register which was placed in the red category as a database which had significant problems and should be revised. Examples of other databases which were included in the red category were the National DNA database, the NHS Detailed Care Record, the Home Office ONSET system, and the Department for Works and Pensions cross-departmental data sharing programme.

Aside from concerns over human rights and protection of privacy, government IT projects have also encountered problems over the introduction of new technology. According to the Parliamentary Office of Science and Technology report on *Government IT Projects* (2003) IT projects in both the public and private sector encounter serious difficulties:

> "Difficulties with IT delivery occur in both the public and private sectors. A survey across sectors found that only 13% of all IT projects, and less than 1% IT development projects, were successful (on time, to specification and to cost)."
> (Parliamentary Office of Science and Technology, 2003: 2)

The report also highlights two surveys on the success of IT projects from 2003, one from the Standish Group and a survey conducted by Oxford University and Computer Weekly which both noted that the success rates for both private and public sector projects were low. The Standish group noted that only a third of the 13,522 IT projects reviewed in America succeeded with nearly 70% being challenged or failing completely.

The Oxford University and Computer Weekly survey found similar problems, noting that one in ten of the IT projects surveyed were abandoned, three quarters of projects were challenged or encountered difficulties, and only 15% of the IT projects succeed. In the context of the National Identity Card Scheme this raise the possibility that even if the scheme is accepted in principle it maybe that in practice the technology fails. The report argues that the reason so many public sector projects fail is that unlike private sector projects they are open to change by policy makers and influence by media reporting of the project. It is further argued that issues of accountability can cause problems with government IT projects:

> "In the private sector, companies are accountable mainly to their shareholders, who may not even be aware of a project's existence. In contrast, the public sector has more open methods of accountability, such as reporting to the National Audit Office and the Public Accounts Committee. It has been suggested that this need for public accountability can lead to a risk averse culture in government, and *EURIM*, the Parliamentary IT lobby group, has recommended replacing, *"the culture of blame avoidance and cover-up followed by witch-hunt by one of risk management with recognition and reward for delivery of outcomes*."
> (Parliamentary Office of Science and Technology, 2003: 9)

When we consider these issues with regard to the identity card scheme it is clear that the influence of both media reporting of the scheme and changes by policy makers have affected the scheme. With concerns over adherence to human rights and privacy legislation it can be argued that these are indicators that the identity card scheme may fail as much in terms of its deployment as in principle. The focus of this study is predominantly on how successful the concept of using an identity card to prevent identity theft and fraud might be. But issues relating to the success of government IT projects in general also raise questions of how successful the identity card scheme might be in practice.

Specific security concerns

The National Identity Card Scheme has also been revised because of specific security concerns, such as the decision to establish several National Identity Registers rather than one centralised register. This change was introduced in order to limit the risk of a single attack by computer hackers providing access to all records stored on the National Identity Register.

Practical security concerns are an area of study with regard to the identity card which will continue to need further study with regard to the identity card as it is conceivable that criminals will develop new ways to adapt to the identity card. The manner and method of how criminals might corrupt or circumvent the ID card is discussed in chapter 9. The insights provided in chapter 9 must be seen as merely the initial concerns as it is likely the interaction between criminals and those administering the identity card will generate even more security issues.

Principle and practice

The aim of this study is to look at the idea of the identity card in principle and with regard to its specific format. The idea that an identity card can be used to prevent identity theft and fraud is something that can be analysed through the study of the perpetration of identity theft and fraud and how it is committed. This will provide an understanding of how forms of identification are manipulated and what impact a single secured form of identification such as the identity card might have. But the specifics of how the scheme is operated will always be open to change. Public opinion, political discourse and the actions of identity thieves will affect the identity card scheme both in the planning stage and when the scheme is brought into effect. This means that there will always be a need to reassess the relationship between the identity card scheme and those involved in committing identity theft. An ideal time to conduct this reassessment would be when the identity card scheme is being introduced so the application process can be examined.

Rather than being able to give a definitive answer as to whether or not the identity card will stop identity theft and fraud, this is the beginning of a prolonged assessment of the identity cards efficacy against current tactics of criminals to defeat the identity card scheme and constraints placed on the scope of the identity card scheme through public protest and political debate.

Internet based research and discourse over the World Wide Web

As part of the planning process for the simulation of identity theft, the internet was used to gather information on how to commit identity theft and how to gather information on someone else. As a source of information the internet proved to be a very valuable resource.

Initially the use of the internet was purely as a means of compiling literature on identity fraud and identity cards. Online archives of newspapers and government reports and statements were downloaded or printed out as a means of supplementing literature from library searches. Over time, it was discovered that there was a far larger body of resources available on the internet on the subjects of identity fraud and identity cards than there was in the local libraries. It became clear that just as the crime of identity fraud was closely associated with the internet, so too the majority of literature on identity fraud and identity cards was internet based.

Accessing information on the internet

Not only were there government websites that gave access to PDF's on identity cards, but there were also private companies like Experian, public interest groups such as the Privacy Rights Clearing House, groups who opposed the introduction of identity cards such as Privacy International, political party websites and web based commentators who shared their views online. The abundance of information on the internet soon eclipsed the information gained from conventional searching of libraries or journals. Even when looking for literature in libraries through the internet it was possible to search online catalogues of various university libraries such as those in London, Manchester and further afield in America and Canada.

Due to the electronic nature of the information gathered a new concern had to be addressed; given that the information obtained came from searches of the internet there arose a risk of being inundated with huge quantities of websites, documents and commentaries from all over the world. Under these circumstances it became necessary to prioritise and organise the information in order to focus on the most relevant.

Through the use of referencing tools such as bookmarks and favourites, it was possible to compile computer files of web addresses stratified along different topic areas. Initially this began with just two files, identity fraud and identity cards, but later this developed further with files on illegal immigration, terrorism, people smuggling and press reports on identity fraud, helping to further stratify the information found on the internet. With regard to identity cards, the internet was used to find any information on related topics and this lead to the creation of additional bookmark tabs on subjects of biometrics and opposition groups. As routinely searching the internet and book marking any useful websites became an important method of gathering information, the book mark files grew, requiring further stratification. The benefit of this was that when it was necessary to research a particular area, for instance illegal immigration, there were already several websites bookmarked as useful sources of information.

This process of book marking websites and gathering information on the internet helped to prioritise the vast amount of information that was available on the internet.
While the process of trawling the internet was time consuming it was still important to distinguish the important or valuable information from the relatively useless.

Discourse over the internet

While there was a large amount of information on the internet which provided insight into identity fraud and identity cards it was still only literature. In order for the role of the internet to be more than the provision of a large store house of information in this research, it was important to use the internet to interact with others. With this in mind, a process was undertaken of using the internet as a means of contacting people who it was

believed would be helpful in answering some more in depth questions about identity fraud and identity cards.

This approach enabled contact with a wide variety of different people and organisations, quickly and without distance being an issue. The issue of distance was a factor as there were a number of people in America who, without the use of the internet, would have been less easily approachable.

Through the internet, access was also gained to university websites and academics who were involved in the study of identity fraud or identity cards. Accessing academics who had a specialty in identity fraud was an important breakthrough in this study. By emailing people like Professor Michael Levi, Dr Natasha Semmens and Dr Emily Finch, it was possible to gain access to papers they had written and they were able to provide direction to others who had expertise in the study of identity fraud. If contact had not been tried with these people through the internet directly, there would have been a reliance on their work coming up during word searches on the internet or searches of online library databases; after seeing the vast amount of information available on the internet this appeared to be more of an issue of luck than skill. Additionally, aside from contacting experts in the field of identity fraud, the internet was also used to contact groups and private organisations involved in identity fraud. There were several organisations in America who were involved in helping victims of identity fraud.

Obtaining confidential information on the internet

Discourse on the subject of identity theft, identity fraud and social engineering was available through searches of web chat rooms and in some instances 'how to' guides can be obtained, explaining how identity fraud can be committed. This is a method of researching identity fraud used previously by journalist Bob Sullivan in his book *Your Evil Twin* (2004), Sullivan noted that information – including credit card numbers, names and addresses and other forms of private information - was available on the internet. This information, according to Sullivan and others, is available through private chat rooms, based in places like Russia and Indonesia. Within the virtual chat rooms

information on people is bought and sold, enabling not only credit card fraud but also larger more complex identity fraud schemes. These chat rooms can often be closed to public contact, requiring a prior relationship with someone who has access to be allowed in. According to Sullivan, aside from these specialist areas of the internet devoted to confidential information stolen from people, a simple web search can provide similar results. The abundance of information available on the internet about people is vast. This is partly due to people's self promotion of their identity, but also because of security leaks at companies charged with protecting information. Equally, there are several easily accessible chat rooms on the internet where people discuss identity theft and manipulation of people to obtain confidential information. Below is an extract of a chat room discourse on social engineering (discussed further in chapter 7) and how to obtain someone's National Insurance number.

> "DISCLAIMER: The information in this post is meant to be used as an educational tool and is intended to be nothing more than a suggestion of theoretical possibilities. I take no responsibility is someone uses the suggestions and information contained in this post to commit fraudulent or illegal acts. I would never and have never condoned these acts, and all the information contained within this post can be found freely available to the public,
>
> Of late, I've noticed a lot of places, including my college, have clamped down significantly on giving people sensitive details over the phone. Kudos to them finally wising up to such things, but it does make life rather annoying and slightly more complicated for us SE's. However, they are still open to convincing e-mails. (I send off single e-mails with a modified e-mail bomber program, allowing me to mimic any email address I need to, but I usually get them to send the details back to me through the post via a drop box.) However, doing it over the phone is just ten times more fun, so try the phone method first, and use the e-mail as a backup, but expect to use it more and more often from now on. Right, now that's out the way, thought I would just drop a couple of pointers for any Brits or anyone who might be doing a little SE in the UK.

Ok, lets start with some basics so that we are all on the same page. In the states, they have Social Security numbers. The UK has exactly the same thing expect we call it a National Insurance number. Now, naturally this number is on the top of most SE's list of useful info.

Now, after a little research I decided to have a little scoot around the HM Revenue & Customs website (they handle taxes and crap) and found that they had rather nicely plunked all their procedural manuals online at http://www.hmrc.gov.uk/manuals/ and they've even ZIPed a lot of them so you can download them. The main website is also packed with juicy details and operating procedures for every single department (including a Departmental Security Manual)

I mean, really.

Amongst downloading and sifting through several bundles of this crap (some of which could prove useful crap in the future) I wandered back through the site and discovered a guide telling you the only people you should give your details too:

- Employers, for the deduction of tax and NICs
- Jobcentre Plus, (Jobs and Benefits in Northern Ireland) to administer Jobseeker's Allowance
- Local Authorities, (The Housing Benefit Executive or the Rates Collection Agency in Northern Ireland), to administer Housing Benefit.
- HM Customs and Excise to administer VAT Registration applications
- Department for Work and Pensions (DWP)

They are basically, in essence, telling you in black and white who you need to be to able to ask for National Insurance numbers. The how, who, where and why I'll leave up to you, but I'll give you an example 'one of my friends' told me about. One day, he was yabbering with his mates in his college cafe when the conversation turned to social engineering. One of his friends laughed the whole notion of social engineering off, saying that real life wasn't like War games or

Sneakers. So, my friend decided it was time to show this guy up and teach him a little lesson. He excused himself and walked outside to the payphone round the corner, dropped a couple of pounds in and called the Colleges front desk.

College: Good Morning Crappy College.

Social Engineer: Good Morning, my names John Smith, I'm calling from the National Insurance Contribution Office of HM Revenue & Service, how are you this morning?

C: I'm fine thanks, and yourself?

SE: I'm fine thank you very much. Basically, I was wondering if you could help me. I'm calling regarding one of your students, would it be possible to check that the person is a registered student at your college?

C: You'll have to talk to Student Services about that, I'll put you through.

After being put through and going through the same introduction and story and request, the lovely lady at Student Services brought the students name up on the computer.

SE: That's great, now would it be possible to just quickly double check some details to make sure they match up with the ones I have here?

The woman on the line paused, and seemed to get a little suspicious.

C: What kind of information?

SE: Just the basics, name, address, NI number, phone number, date of birth, just so I can verify that they are who they say they are.

She seemed to swallow that.

C: Ok, do you want me to just read them off now?

SE: If you can now, if not you can simply email them to me.

This wasn't bullshit; they had set up an email with a @hmrc.co.uk domain.

Luckily, she just read them all out and my friend wrote them down. Couple of minutes later, my friend returned to the college cafe and passed the paper, complete with all this guys 'private details' on. His face must have been a picture. Well, that's my say, its a little crude and simple but it can work. All I can say is before you do anything; research, research, research. And then, research again.

Then revise and research. Remember, this aint exactly legal, so either don't get caught, or don't do it at all.
PS If there are some screw ups in this, please feel free to flame me. You gotta learn from yah mistakes, right?(/code)
Last edited by PP on Thu Nov 30, 2006 9:24 pm; edited 1 time in total"
(Anon, Social Engineers 101, 2006: 1-2)

This web chat room was devoted to social engineering and the methods of how to manipulate people through lying and pretexting. The people who frequented this site discussed their own experiences and successes. These accounts implied that through simple observation, research and the confidence to try, people can be manipulated into divulging confidential information.

An alternative name for social engineering is pretexting; this is a practice used by private investigators and those involved in information brokering. It is possible that the approaches discussed do not work or that claims of success by chat room users are false. But while it may be a mistake to take these accounts as completely truthful, they do highlight the way social engineering involves asserting a claim for information or identification by falsely claiming a right to that information.

From this chat room, it also became clear that the majority of discussion was on social engineering in the U.S.A. Aside from the above example, most discourse between social engineers was of exploits carried out in the U.S.A. The majority of people in this chat room referred to obtaining the types of identification commonly found in America – Social Security Numbers, State Drivers Licences etc.

The aim of this study was to investigate identity theft and fraud in the U.K. and aside from a few contributions from people in the U.K. (or at least people who claim to be from the U.K.) there was very little discussion of the situation in the U.K. This is in part to be expected, as the phenomenon of identity fraud has been a widely discussed issue in the U.S.A. for the last fifteen years (See chapter 3). Identity fraud has only received an

increased coverage in the U.K. media since the millennium. In time, it may be that there will be an increased interest in social engineering in the U.K.

Training available on the Internet

As well as individuals discussing their own experiences on the internet there is also a number of websites where training information can be obtained on how to steal identities or learn the skills of social engineering. These guides often come with disclaimers against their use by criminals but do in themselves discuss the ease with which the law can be broken using the techniques they describe.

Information in America

As discussed in chapter 3, identity theft is an issue which has received a great deal of attention in America. Consequently there are several organisations and individuals in America with useful information on the subject of identity theft. Through the internet it was possible to contact these groups and individuals in order to gain insight into identity theft and identity fraud. One of the first groups contacted who specialise in identity theft was the Privacy Rights Clearing House group. This group is a key organisation in the formation of the identity theft law in the U.S.A. and they were contacted directly with this email:

> "Hello
> My name is Tim Holmes I am a researcher at the University of Wales Bangor. I am conducting a study into id fraud in the U.K and the possible impact of an id card system on this type of crime.
> I was hoping you could help me, as part of my study I am looking in to identity fraud in America, in particular when did identity fraud/identity theft become a big issue in America, and how has your country responded.
> Any help you could give my study would be greatly appreciated.
> Regards
> Tim Holmes" (Holmes.T, 2006 see appendix 8 for original email)

This email is a general introduction used when contacting organisations via email. This contact was an important one to make as prior research into identity theft in America had revealed the importance of the Privacy Rights Clearing House as a source of information and expertise. Luckily, through this contact it was possible to access not only information on identity theft in America but also contact information for other experts on identity theft. This is the response received from the Privacy Rights Clearing House's director Beth Givens:

> "I wish I had the answers to your questions in a single document -- or I could point you to a history of id theft in the U.S. Unfortunately, I don't have such a document at my fingertips. And to give you my assessment would take more time than I have, sorry to say. It's a big topic. The first hearing on the topic was held by the Federal Trade Commission in 1996. You might be able to find some useful info in the materials associated with that hearing (they call their hearings workshops). I believe you'll find the transcripts here:
> http://www.ftc.gov/bcp/workshops/idtheft/index.html
> Here are some links that you might find useful for older materials:
> http://www.ftc.gov/os/1998/05/identhef.htm
> http://www.ftc.gov/os/1998/05/identhef.htm
> And we have a page that links you to various id theft surveys:
> http://www.privacyrights.org/ar/idtheftsurveys.htm
> Good luck!
> Beth Givens" (Givens.B, 2006 see appendix 9 for original email)

After this initial response was received a follow up email was sent, the goal of which was to discuss academic research in America:

> "Hi
> Thanks for responding to my e-mail. I am about to look through the

stuff you have sent me. I would have liked a big history of id theft in the U.S but I am not surprised that it isn't easy to find. From my research I have found that id theft/id fraud is a subject which generally doesn't receive much academic attention or research.
(Apart from the U.S and the U.K the only other place in the world that looks at Id fraud is Australia)

Thanks for the information

All the Best

Tim Holmes" (Holmes.T, 2006 see appendix 10 for original email)

Givens responded with an email that directed me to experts in America on identity theft:

"I know of a PhD student who is studying id theft for her dissertation. She's from Rutgers Univ and is visiting my office later this week.
Her contact info is:

Megan McNally

Perhaps she has run across a general history of the subject.
Another possible resource is Judith Collins, PhD, of Michigan State Univ. She has established an id theft center
Good luck!" (Givens.B, 2006 see appendix 11 for original email)

Through this email it was possible to contact Megan McNally, the PhD student. This connection proved very useful as McNally is very knowledgeable about identity theft in America. Over a period of several months it was possible to discuss via email with McNally several ideas and theories on identity and identity theft. This discourse helped to refine and improve theories and understanding with regard to the subject of identity and identity theft. (See appendix 12 for examples)

As well as seeking out others to discuss identity fraud within America, contact was made with several of the organisations in America devoted to helping victims of identity fraud. These groups provide information and the opportunity to discuss identity fraud with experts; however it became clear that the information received was specific to the

U.S.A. While researching identity fraud in America was useful in providing background material, it was evident that there was a need for research specific to the U.K.

Can you trust the internet?

This discourse was only achievable thanks to the internet, but it also raised several questions over the nature of identity. There has never been a face-to-face meeting with Megan McNally and despite a quick search of the Rutgers University website a picture of her was unavailable nor was there much in the way of biographical information beyond what has been said in our emails. Not much is really know about her in the traditional sense of identification beyond text from emails and whatever inferences could be drawn from them as to what kind of person she may be.

The internet as a whole, aside from being a huge technological endeavour, is also an exercise in trust and assumption. It was assumed that the people spoken to are who they claim to be and are in a position to speak effectively and accurately on behalf of their organisation. Ultimately, for this study, it is only possible to trust that the information obtained is accurate and genuine.

It is possible to criticise research or information gathered over the internet because of the lack of guarantee as to accuracy and reliability. This study looks at several methods of impersonation and counterfeiting on the internet. So how much trust and value should be placed in the information given over and through the internet?

It can be argued that, at least if there had been a meeting with these people face-to-face, it could have brought another element of identification and judgement into play. But equally, as this study of identity fraud in face-to-face encounters will show, even in face-to-face encounters there are incidents where people have been deceived.

In researching what is essentially lying, the issue of what information can be trusted and what appears to be reliable is open to a great deal of personal interpretation. In this study, it has been necessary to reason that there is a possibility that someone may have been lying, that the people spoken to over the internet are not who they claim to be.

Nevertheless there can be no guarantee that the information provided here is accurate or true; ultimately this entire endeavour could be a fabrication, and this study, like the information used in it, is dependant on readers trusting its authenticity and their ability to discern truth from lies.

CHAPTER 6

History of Identity Related Crime

Origins of identity fraud and identity theft

In attempting to establish the origins of the crimes of identity theft and identity fraud, it is important to deconstruct the implicit meaning behind these terms. As discussed in chapters 2 and 3, the terms identity and fraud are open to as much interpretation as the concept of identity fraud itself. There is no cast-iron definition of identity; it is a contentious term that refers to issues of categorisation by the individual and society, personality, role in society, self presentation, social symbolism and bonds of both personal and social trust. The issue of defining an identity is further complicated when trying to define what it means to lie about an identity.

It can be argued that all crimes which involve some degree of deception involve a person's identity and society's efforts to identify them. A liar wants to be perceived as a truthful person; a bank robber who conceals his face wants to avoid being labelled as a criminal. Crimes of deception are incidents where criminals succeed by providing a false representation of who they are, how trust worthy they are, and their intentions. All of these are, in a sense, elements of a person's identity. It can therefore be argued that all crimes of deception - *all fraud* - is identity fraud, as all involve false representation and misidentification.

The issue is no less problematic if the term theft is used; the term identity theft implies that something is taken away. However victims are often is able to continue using their identity after the theft, and in some cases may be unaware they are a victims at all. It is also worth asking what is actually taken in cases of identity theft. If it is information, how can we claim ownership of such facts? In order to be a part of our identity, details about who we are must be shared with society and open to modification by society. It can further be argued that any unwanted modification of our identities by other individuals within society can be a form of identity theft. In a very broad interpretation of identity theft, it can be argued that someone who is victimised by any form of

criminal activity is in effect a victim of identity theft as they are forced to exchange the identity of non-victim for that of victim. In effect their identity is altered against their will, and positive aspects of who they are (be it psychological, financial, material etc.) are taken from them. Thus if we look at the concepts of identity fraud and identity theft in these very broad terms they become meaningless. While discussion of the use of deception and impersonation is important when defining identity fraud and identity theft, an explanation of these forms of criminal activity should not be based on these criteria alone.

When defining identity fraud and identity theft, another aspect of the identification process must be considered, namely the formation of bonds of trust. Anyone can lie about who they are, or even impersonate another person, but what turns these deceptions into acts of identity fraud and identity theft are the bonds of trust they break. By focusing on which bonds of trust are breached and to what extent it is possible to use the terms identity fraud and identity theft in a more effective manner, they become less about the act of lying and more about the manner and consequence of the lies told.

While the terms identity theft and identity fraud will be explained in detail in the next two chapters, the emphasis of this chapter is the history of identity related crime. In order to put the timeline presented here in context the crimes of identity fraud and identity theft are defined thus:

Identity theft – the impersonation of a specific person's personal identity victimising an individual, and their presentation of self. The act of identity theft can and often does lead to a further instance of identity fraud (see chapter 8 & 9 for more). The emphasis here on impersonating a person's personal identity and benefit from victimising that person.

Identity fraud – deception, either through the use of a false or stolen identity victimising society and its trust in a person's social role and/or social status. The emphasis here is on abusing individuals in society by deceiving them as to who the identity fraudster is.

The timelines presented in this chapter show how identity related crime can be distinguished in terms of who is being victimised and how. Looking at the history of identity related crime there are two connected histories, the history of identity fraud and the history of identity theft.

Communicating identity over distance and forming bonds of trust

Looking at the history of both identity fraud and identity theft, an important element to consider is the value of an individual's personal identity. Current concerns about identity theft and identity fraud are based predominantly upon the risks faced by the general public from these crimes. This risk is however a new phenomenon, as changes in-+ technology and culture in western society have altered the value of a person's personal identity.

Today it is possible to communicate and express one's personal identity on a global scale through technology such as the internet; in previous century's individuals' ability to communicate who they are (or who they are impersonating) was limited.

The history of identity related crime shows the development of personal identities and the influence of this on the activities of professional criminals. In this chapter, it will be argued that the majority of early identity related crimes focused on deception rather than impersonation. Identity fraud has been favoured over identity theft because of the relatively limited value of impersonating an individual's personal identity.

The history of identity fraud

As noted above, identity fraud is the action of deceiving someone as to one's true social status or role in society. Historically, there have been several cases of fraud where people have deceived others as to their social status or role. In one of the earliest forms

of advanced fee fraud – that of the Spanish Prisoner (Ampratwum 2009) - the success of the crime is dependent on successfully deceiving the victim as to their status as a representative of the king.

The Spanish Prisoner is one of the oldest confidence games and originates from 1588. The scam begins with a criminal pretending to be a representative of the king and approaching the victim. The criminal explains to the victim that a prince – travelling in disguise – has been captured by the Spanish and is being held hostage. The criminal goes on to explain that the Spanish are unaware that the man they are holding hostage is actually a prince. Consequently, an opportunity exists for the king to pay a smaller ransom for the prince than he would otherwise need to. In order to do this, the criminal explains, the king needs someone else to pay the smaller ransom; so the Spanish do not become suspicious as to why the king would be willing to pay the ransom for someone the Spanish consider to be of little value. This is where the victim comes in: the criminal tells them the king needs the victim to pay the ransom. Once the Spanish prisoner is returned, the criminal tells the victim that the king will repay the victim a larger sum than the victim paid to secure the release of the Spanish Prisoner. As well as the promise of a larger sum of money than the victim had to provide for the ransom, the victim is also promised some form of increase in social status. In effect, the victim is asked to give the criminal a sum of money on the promise that the victim will receive a larger reward later. After the victims have handed over the money, they are informed that there have been complications and that more money is needed; the victim is then routinely told that there is a need for them to give more money. The scam ends when the victim has no more money.

The Nigerian 419 scam is a more up to date version of advanced fee fraud which follows many of the same principles as the Spanish Prisoner, in both it is misrepresentation rather than impersonation of people that enables the fraud. Older forms of fraud using fake and false information, information without any official involvement or confirmation, are still used today on the internet where the large number of potential victims and lack of security make this type of crime still viable.

Below are three examples of a scam which use the Nigerian 419 model in order to show the similarity in techniques. As with any scam of this type, the aim is to elicit sympathy from the victim and the belief there will be financial gain; all that is required is an initial amount of money from the victim. A common tactic in this type of scam is to use a well publicised event or situation the victim will know about such as a large scale lottery, or situation that has recently received media attention and in which people need help, for example a natural disaster such as the South East Asia Tsunami. The first example is of a Nigerian 419 scam:

From: rose williams.
Abidjan Cote d' ivoire
West Africa.

Dearest One,

Good day to you.

My name is Miss rose williams and am 19 years old. Is my pleasure sending you this message. I am requesting you to go through it carefully and get back to me the soonest.

I am contactacting you for a business venture which I intend to establish in your country. Though we have not met before, I firmly believe, that you will not lead me astray after fervent prayers and fasting.

There is this huge amount of nine million five hundred thousand U.S dollars ($9.5m) which my late Father Mr. Albert wiliams deposited for me in a Security Company here in Abidjan before he was assassinated by unknown persons during the war in our country Cote d'ivoire. He intentionally deposited it as family valuables for its safe keeping in the Security Company.

Now, I have decided to invest this money in your country or anywhere safe enough outside Africa for security and political reasons. I want you to assist me claim and retrieve this fund from the Security Company and transfer it into your personal account in your country for investment. I will cheerish it if you can

consider these listed areas below for the investment.

1). Telecommunication.

2). The Transport Industry.

3). Five Star Hotel.

I will be pleased and grateful offering you 20% of the total fund as compensation for your kind gesture and assistance. God bless you and i await your soonest response.

Yours Faithfully,

Miss rose .williams (see appendix 13 for original email)

This next example uses the current problems in Zimbabwe:

My Dear Friend,

This letter might come to you as a surprise as we have not met before, but I believe that you would be compelled to help me after going through the contents of this letter. My name is Maria Del Carmen Stevens a swedish, my meeting with Mr David Yendall Stevens in south africa led us into marriage. my husband Mr David stevens who is now late farmer and exporter of Tobacco in the Republic of Zimbabwe, he was shot dead allegedly by ZANU-PF supporters in zimbabwe on 25th of april 2000 in the farm. You can confirm this by copying and pasting this link on your internet browser.or click on it:
http://news.bbc.co.uk/1/hi/world/africa/725643.stm,
http://news.bbc.co.uk/1/hi/world/africa/818766.stm

He (Robert Mugabe) did not stop at that; he also went on to expel all White farmers in Zimbabwe. He implored the services of his war veterans to undertake this seizure. The war veterans have been accused (correctly) of being behind the

violent occupation of white-owned commercial farms in which an estimated 70,000 farm workers have been displaced. At least, over hundreds white farmers and black settlers have been killed since the farm invasions began in February 2000.We have decided that we must see this problem to the end.

Although we know that we are taking a great risk by staying here in Zimbabwe. At the Moment, our phone lines are bugged, and all our movements are being monitored by Zimbabwe's (Robert Mugabe)secret Police. Therefore email is the safest means of communication for now.
We (White farmers in Zimbabwe) have taken our case to the United Nations and even with the threats of transactions and the subsequent sanctions from the West against the Zimbabwean Authorities, Robert Mugabe (The president of Zimbabwe) still remains adamant.
He is insisting that our farm land (some of which we bought with our money and most of which We inherited from our fathers) belongs to the (his) government of Zimbabwe.the government of zimbabwe has asked all white-farmers to give up their farms to black farmers or risk going to prison. So far, more than 1,400 white owned farms have been invaded and confiscated, as well as claiming the properties of the farmers.Also, about 133 white farmers were arrested for defying the orders to leave their farms under the controversial land reform program of the government,

Since I could not keep the money in Zimbabwe, I used the services of a Diplomatic Courier Company to move this money (registered as official documents) out of Zimbabwe to Europe. At present, my money totaling US$28,750,000. (Twenty eight million, seven hundred and fifty thousand United States Dollars) is in Europe and hopefully, it would be paid into an offshore account. Can you help me? Are you trustworthy? Can you handle this money? Are you capable of handling this money? If you can, please contact me. All you need to do is to claim this money from the Courier Company.

You will be required to contact the Courier Company that moved this money (official documents) out of Zimbabwe to Europe. All necessary particulars which can facilitate and enable you claim the money on my behalf will be forwarded to you as soon as your consent to proceed is received. For your assistance you will be entitled to have 20% of the total sum. You are also obliged to help/advise on the proper and most convenient way of investing this money in your country, Hopefully, You will consider this request and respond positively.

Yours Sincerely,
Maria Stevens (see appendix 14 for original email)

Below is the third example of a 419 'scam'; again, there is discussion of a situation which requires the victim's input to secure a large sum of money:

Hello,

I AM MR Paul Cooper,A SOUTH AFRICAN working with SENEGAL BRANCH OF CREDIT MUTUAL DU SENEGAL AS THE MANAGER.My apologies if you find my mail intruding, i do not intend to offend you but only wish to use this medium to propose a business transaction to you which i believe would be of financial benefits to both of us if you agree to work with me.

First,i would like you to know that i would understand if you take this proposal to be some scam or hoax as i would probably think the same in your place. I also receive a lot of spam mails all the time which to be honest with you is how i got the idea of contacting you through this medium from.I want to assure you this is a real and genuine business.

I am sorry,i can only give you a few details of the transaction at this moment as i am not sure of your position yet and would not want to risk destroying everything i have worked hard for so far by being carefree and disclosing vital

information's at this point that could get me into trouble,i have to be sure you are willing to work with me before i can give you the full details including my personal information's.

The total amount involved is around NINE MILLION UNITED STATES OF AMERICA DOLLARS and all i need from you is to help me get the funds over to you safely, i have everything all worked out and there would be no risk or danger in this transaction.

If you are willing to co-operate with me on this deal feel free to give me a call or write me ASAP indicating your sincere interest and for further information's and any questions you might wish to ask me. Thanks for your time and i look forward to a positive response from you soon.

Thanks,
Paul Cooper (see appendix 15 for original email)

These examples refer to different situations, but both also involve a large sum of money that requires the assistance of another person to secure, the other person being the victim, who if they respond will be informed that they will have to give a sum of money to help secure the larger sum of money.

These examples represent a type of advance fee fraud which is dependent on providing a persona that people will trust and sympathise with, to the point they will be willing to enter into a business arrangement. The use of identity in the Spanish Prisoner, and its modern version in the Nigerian 419 scams, focuses on abusing the bond of trust people form with other members of society. The identity abused in this instance is the general process of identification and social trust we all use when interacting with others.

The formation of a more general identity of someone who can be trusted is an activity many professional con artists have used over the years. The term con artist is derived from a report in the New York Herald (1849) on the activities of a 19th century thief

William Thompson. Thompson was known as the Confidence Man because of the approach he took to stealing people's property:

> "...he would go up to a perfect stranger in the street, and being a man of genteel appearance, would easily command an interview. Upon this interview he would say after some little conversation, 'have you confidence in me to trust me with your watch until to-morrow;' the stranger at this novel request, supposing him to be some old acquaintance not at the moment recollected, allows him to take the watch, thus placing 'confidence' in the honesty of a strange, who walks off laughing and the other supposing it to be a joke allows him so to do." (New York Herald, July 8th 1849: 1)

The case of William Thompson is important not only in the establishment of the term 'confidence man'. This case also shows how identity fraud does not necessarily involve using a false name or personal identity; all that is required is identification as someone with the appropriate social status or role.

This practice of establishing a trustworthy identity has been utilised by several subsequent con men. For example, there have been con artists such as Arthur Ferguson who during the 1920s conned several American tourists into buying famous London monuments, and Victor Lustig who in 1925 sold the Eiffel Tower to a Parisian scrap merchant who have defrauded people by impersonating official representatives of governments.

Use of appearance and group identities in identity fraud

As seen in several of the examples above, the use of general identities by con artists has been a tried and tested method of committing identity fraud. It can be argued that focusing on an individual and their personal identity is a modern trend. The use of identity fraud does not require the criminals to lie about their names (although they can and sometimes do) or to abuse another individual's identity directly rather; it involves stealing an archetypal or general identity. Examples of the theft of archetypal identities

include people who have impersonated members of state organisations such as the police or the armed forces, or private organisations. Another aspect of identity fraud is deception with regard to social groupings such as ethnicity or gender.

Often these groups have some requirements for entry; their worthiness to claim to be member of organisations has to be judged. Once entry to the group is achieved, there is often some way to distinguish a member of that group from the rest of society. As discussed in chapter 2 a common method is the use of dress or social symbolism through badges or documentation. In incidents of group identity theft the process of being accepted into the group is circumvented and, wherever possible, the identity theft accesses the social symbols which distinguish a member of that group from the rest of society.

The focus of modern identity theft and fraud has been on individuals and the social symbols which distinguish them from the rest of society. It is the victimisation of a single person's identity that has raised public concern over this crime. But it can be argued that identity theft aimed at one person is simply a specialised form of a larger area of fraudulent activity and that identity fraud can be committed without victimising an individual.

Below are several examples of identity fraud which have not involved the impersonation of another person or the theft of their identity. The following examples of identity fraud are crimes which have involved deception by claiming membership of social groups or organisations.

Identity fraud and the army

One area where there have been several instances of people falsely claiming membership of a social group involves individuals who have claimed to be members of military organisations.

In America there have been several incidents of men falsely claiming to have been members of elite military and covert government organisations and there has been a great deal of attention given to people who impersonate members of one elite group in the U.S. armed forces, the U.S. Navy Seals. This is one of the most elite military forces in America and has been in existence since the Vietnam War. Becoming a U.S. Navy Seal is very difficult and there is much secrecy surrounding the identity of the Navy Seals, and their activities. Often the activities of this group are kept secret, and as a by-product of this it can be easy to claim to be a former member of this organisation. If challenged, impostors can claim that their activities and membership of the Seals is classified information. In order to combat 'phony seals', a number of genuine retired seals have taken it upon themselves to investigate possible impersonators:

> "Phony seals?? Fake seals?? Wannabe Seals??
> Different names, yet the same kind of 'animal'!!
> They are pretenders who claim they have seen Vietnam UDT/SEAL action, Top secret/covert action, and/or even antiterrorist RED CELL, and/or SEAL team 6 missions 'they can't disclose' and any other heroic {hah!} SPECWAR Team action{s}!! Mostly, you can recognize them: they wear SEAL/UDT patches, Trident Insignias, Black Berets, Cammo's, even they go so far as to carry or possess Naval Weapons! They talk big!" (Nightscribe.com, 2007: 1)

According to this website there are several reasons for impersonating a Navy Seal: impersonators can use their claim to make money giving personal appearances, speeches, publishing and as part of their employment background to gain eligibility for future employment. However, while there is the possibility of defrauding others through this impersonation, its greater significance to genuine members of the U.S. Navy Seals is the 'disrespect' to their status that they perceive. Some have used impersonation of military personnel for financial gain. However, the impersonation of military personnel has been carried out for other reasons. Claiming to be a member of an elite military force can be an aspect of a mental illness. Here someone has a false view of themselves and their own identity. An example of this kind of person would be Barry George, the

man falsely convicted of the 1999 murder of T.V. presenter Jill Dando. The trial process and subsequent appeals revealed a great deal about Mr George and false claims he had made. It was reported by the BBC (2008), that the trial and appeals process surrounding George's conviction for Dando's murder revealed how George had made several false claims about who he was. In the years leading up to the death of Jill Dando, George had used several aliases and other people's identities. For example, he had for a time claimed to be Thomas Palmer, a member of the S.A.S. who was involved in the Iranian embassy siege in 1980.George had obtained copies of Palmer's birth and marriage certificates and opened a building society account in his name. George's mental condition became an issue in the appeal process, with his defence team citing a personality disorder and a low I.Q. as a reason why George could not have killed Jill Dando. It was argued that George was in many respects a man with a limited grasp on reality. The claim of membership of the military and elite groups within the armed forces as a form of identification, in this example, is as a means of fulfilling a fantasy or establishing a self image. In the story *'The Secret life of Walter Mitty'* by James Thurber (1939), a similar scenario is discussed. In this story the main protagonist, Walter Mitty fantasises about being, among other things, a Navy captain, a fighter pilot, and a world famous doctor, as a way of escaping his boring life. Referring to someone as being like Walter Mitty has become a way to imply that that person is in some way delusional.

Instead of from falsely claiming to be a member of the armed forces for financial reasons, or as part of a mental illness, some have used impersonation of military personnel to gain publicity and fame. In a recent effort to protest against the war in Iraq, a man impersonated a soldier in order to criticise the activities of the U.S. army in Iraq. In a 20 minute video interview, Jesse Macbeth explains how he and other soldiers were ordered to terrorise and abuse Iraqi locals:

"By my hand alone.... Almost 200 people were taken out by me. That's just a rough estimate. A lot of them at close range... they would actually feel the hot muzzle of my rifle on their forehead... we'd do stuff that would scare them first... beat'em up or kick 'em or hit the wife... slaughtering 30-40 people a

> night sometimes, women and children... I was trained, you know, in all the Ranger school, 18 months of that crap... I got disappointed in my country... but I didn't say anything because I would have been locked up." (Malkin .M, 2006: 1)

Soon after the interview with Jesse Macbeth had been televised on the internet, the U.S. Department of the Army reported that Macbeth had not been in the army. Furthermore, groups of web bloggers with knowledge of the army on the internet began to debunk Macbeth's story. Discrepancies and inconsistencies in Macbeth's story were highlighted Macbeth had claimed that he had joined the army at 16 and left when he was 20, that he had been injured several times and that he had served in the U.S. Army Rangers and in the U.S. Special Forces. Another major discrepancy was discovered in a photograph of Macbeth in his uniform which was missing several key details (various badges and insignia), and his beret was back to front.

Another incident of someone pretending to be a member of the U.S army came to light in 2004. Micah Ian Wright had claimed to be a veteran of the 1989 Panama invasion and a former member of the U.S. Army Rangers. Due to his experiences in that conflict, Wright had become an anti war protestor and had written a book *"You Back the Attack! We'll Bomb Who We Want!"*. However, when the Washington Post began an investigation into Wright, it was discovered that he had never served in the army. Upon his discovery, Wright was compelled to write an apology on his website:

> "Hi My name is Micah Wright. I'm a former Army Ranger, and I've been lying to you. I've kept the secret for years now, but all lies grow and eventually get out of control. This is me coming clean about my Big Lie. What did I lie about? Oh, nothing much... Except that I was never an Army Ranger. I never served a day in a Ranger Regiment. I never went to Ranger School. The closest I ever got was Army ROTC." (Wright .M, 2004: 1)

Wright goes on to explain that while he had never served in the army there was a lingering perception amongst his friends that he had at some time been an army ranger. According to Wright, he began spreading the story that he had served in Panama after the terrorist attacks in America on September 11th 2001. After the terrorist attacks, Wright wrote a book which included World War Two propaganda posters with altered text which included criticism of the U.S. government's 'War on Terror'. Wright goes on to explain that the response to his book included several claims that his work amounted to treason and Wright received several death threats. In order to counteract the impression that he was in some way 'un-American', Wright resurrected the lie that he had been in the army and devised a story about how he had served in the Rangers during the invasion of Panama and had parachuted behind enemy lines during the conflict. The actions of people like Macbeth and Wright are, arguably, variations on the crime of identity fraud in as much as they have adopted a form of identification to which they are not entitled. Another aspect of identity fraud involving the military is the use of identity fraud by war criminals.

Use of identity fraud by war criminals

After the Second World War, several high ranking Nazi war criminals, people such as Henrich Himmler, Adolf Eichmann and Josef Mengele used false identities to avoid capture and prosecution for war crimes. Himmler attempted to avoid capture by the Allies by assuming a false identity, but he was eventually captured. Eichmann was able to hide in Germany for a time before he moved first to Italy and then to Argentina. Similarly, Josef Mengele made his way to Argentina after hiding in Germany.

One of the reasons these men were able to escape from Germany was that there were several organisations who intentionally and unintentionally aided their efforts. Aside from ODESSA (Organisation der SS Angehoerigen-Association of SS Members) which actively tried to help Nazis escape, other organisations such as the International Red Cross inadvertently aided the escape to South America by Eichmann and Mengele and other Nazi war criminals to by providing them with travel documents when they were hiding in refugee camps.

Many Nazi war criminals headed for South America and countries such as Argentina. Argentina was a good choice for Nazis from Germany because the leader at the time. Juan Peron was a right wing leader who had cultivated strong ties with Germany and the expatriate German community who lived in Argentina. During the 1950s and 1960s the government of Israel and individuals such as Simon Wiesenthal sought to find Nazi War criminals living under false identities in South America.

There is the case of Adolf Eichmann - the man who was in charge of the final solution to the Jewish question which involved the organising of the concentration camps and the execution of European Jews. Eichmann's activities after the war are discussed by Smart (2009) who notes that Eichmann was able through a series of false identities to reach South America and avoid the prosecution of the war crimes court established in Nuremberg. Unlike Mengele who was able to hide in a farmhouse near Gunzberg until he could escape to Argentina (Bulow, 2008), Eichmann had to use a variety of false identities in order to escape. Initially Eichmann pretended to be a Luftwaffe (German Air Force) airman called Adolf Karl Barth in order to avoid capture. While pretending to be Barth, Eichmann was caught and put in a prisoner of war camp where he used the name Otto Eckmann. Eichmann eventually escaped and, using the identity of a forest ranger called Otto Heninger, made his way through Austria to Italy with the help of the O.D.E.S.S.A. network; once in Italy Eichmann was able to escape to Argentina.

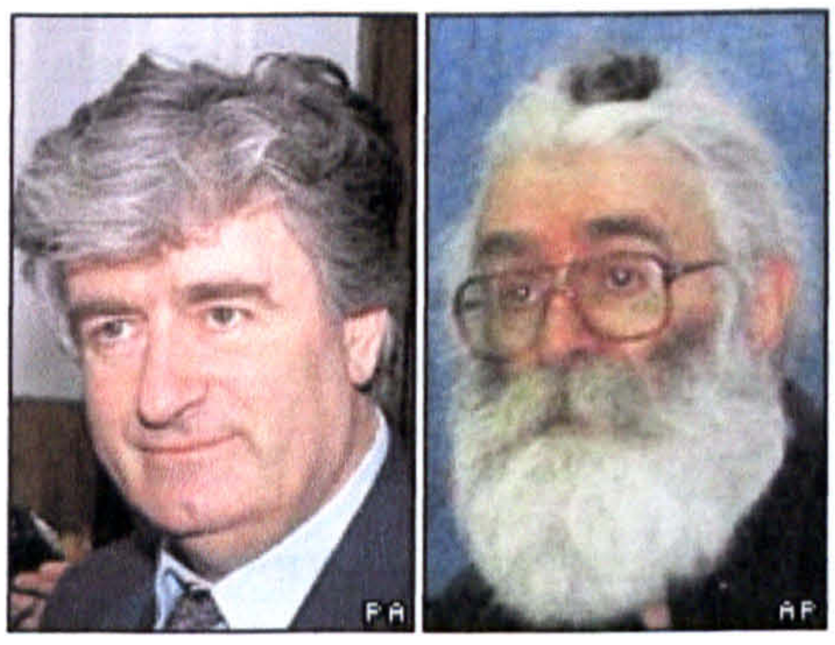
In 1952, Adolf Eichmann was living under the name Ricardo Klement in Argentina. Eichmann claimed to be a mechanic and was employed as a labour organiser by the Capri Construction, Measurements and Waterworks Company which sheltered many war criminals. By 1961, Eichmann had been captured by Israeli agents and transported to Israel where he was put on trial for his actions during the war. In 1962 he was hanged.

The use of false or stolen identities as a means of avoiding detection by the police or authorities has been utilized by a number of people suspected or wanted for crimes since the Second World War. Most notable are cases of suspected Serbian war criminals in

which false identities have been used to avoid prosecution at the International War Crimes Tribunal held at the Hague in the Netherlands. One example is Vlastimir Djordjevic who was accused of ordering the killing of Kosovo Albanians. According to the South Eastern Europe Times (2007), Djordjevic had been living in Budva under a false identity as Novica Karadzic since 2004. He had grown a beard and was employed as a construction worker there for more than two months.

In 2008, former Bosnian Serb leader and wanted war criminal Radovan Karadzic was discovered in Belgrade after ten years on the run. Over these ten years, Karadzic had grown a long white beard and used the false identity, Dragan Dabic. As Dragan Dabic, Karadzic practised alternative medicine, according to the BBC (2008):

> "Masquerading as an expert in human quantum energy, the fugitive was so confident in his disguise he even had his own website, and would give out business cards during alternative medicine lectures." (BBC News, 2008: 1)



left Karadzic ten years ago, right Karadzic today (BBC News, 2008: 1)

In the Second World War cases discussed above, the war criminals often attempted to avoid prosecution by moving far away from their homelands. Karadzic, in contrast, stayed close to home and was apparently able to completely deceive the people around him, despite his notoriety.

Identity fraud and espionage

Deception with regard to identity is also used in instances of espionage. This is an area of activity which can be difficult to research. The use of false identities by spies has been a well publicized phenomenon in fiction, and in real life there are also several accounts of false identities being used by the police and the security services of various countries. While it is difficult to find specific information on how false identities are used in cases of espionage, or as part of covert police investigations, there are some historical accounts we can refer to.

In a report for the Guardian by Taylor (2002), the use of false identities by undercover police officers from the 1960s to the 1980s is discussed. Taylor's report focuses on the experiences of the 'Hairies', a squad of undercover police officers. The name 'Hairies' was given to the squad because of their habit of growing their hair out from the usual short haircut of police officers, and in some instances growing beards in order to improve their chances of deceiving people. Apart from changing their appearance, it was also a common practice for the 'Hairies' to adopt a new identity, which they referred to as 'legend':

> "Each hairy worked out his own legend and memorised. Richard had just read 'The Day of the Jackal' and decided to adopt a new persona like Frederick Forsyth's assassin the identity of someone who had died young. 'I spent weeks and weeks at St Catherine's House studying birth and death records. I was looking for child who'd been born about the same time as myself and died soon after. I found him and resurrected him.' Richard visited the town where the boy who was providing his cover was born – and from which the family had conveniently moved away – and researched every detail of the family's history."
> (Taylor .P, 2002: 1)

The approaches to formulating legends varied, according to Taylor, but one common theme in all accounts was the need to establish something more than a paper proof of identity. There was a need to prove not only the 'legend' through the use of

documentation, but also to demonstrate that the undercover officer was also living that life on a daily basis. This practice can be seen as a form of partial or wholesale assumption which is discussed further in chapter 8. The use of a dead person's identity is also discussed further in the account of Charles Stopford's use of Christopher Buckingham's identity on page 115.

Another example of the use of false identities in espionage is the attempt of two Israeli men who in 2004 were imprisoned in New Zealand for attempting to obtain passports from that country. After the suspicions of a passport officer were raised, authorities investigated and found a conspiracy involving four Mossad agents, (from the Israeli secret service) who were attempting to set up a false identity for an agent called Zev Barkan. Only two of the four were caught, Uriel Kelman and Eli Cara, and when both appeared in court in 2004 they went to extraordinary lengths to try to conceal their identities: Kelman wore a balaclava while Cara had changed his hair colour and attempted to alter his appearance. Their conspiracy involved setting up a fake travel agency and trying to steal the identity of a wheelchair bound man. Their goal was to obtain a passport in this man's name. The use of false identities and documentation by Mossad has taken place before; in 1997, Mossad used a fake Canadian passport when they attempted to set up an operation to assassinate Sheikh Khaled Mashal a leader of Hamas.

Identity fraud and the medical profession

There have been several cases of people obtaining false qualifications and impersonating doctors. In many cases, the actions of these individuals involved the development of fake documentation or the use of another person's legitimate accreditation.

According to Lister (2005) one major case of this type of identity fraud was when a man called Barian Baluchi posed as an expert in psychiatric care for refugees, neuropsychiatry, plastic surgery and post traumatic stress. Under this guise, Baluchi (a taxi driver) emigrated to the U.K. and began impersonating a Madrid based psychiatrist

called Antonio Carrillo-Gomez. Baluchi was able to pass himself off as an expert in asylum seekers and refugees and he gave evidence in court and signed 1,500 reports on asylum seekers,1,000 of whom were allowed to stay in the U.K. As a fake doctor, Baluchi made more than £1.5 million from various charities, grants, local councils and the Departments of Health and the Home Office.

The case of Mr Baluchi is not an isolated one; in 1998 Godwin Onubogu was found to have been impersonating a doctor for over a decade. Onubogu was a laboratory technician; after taking an Open University Science Foundation Course and working in a London based laboratory, he setup his own laboratory testing company called Iketam Clinical Laboratory Services with the help of an enterprise agency grant. According to Louise Kamill who prosecuted Onubogu:

> "All he wanted to do was to call himself doctor. He clearly thought of degrees as only a formality" (Kamil cited in BBC News, 1998: 1)

Onubogu used his laboratory to see 400 people as patients; he used fake medical qualifications, pictures of himself in academic robes and fake medical articles. Onubogu, like Baluchi also used his pretence to appear as a medical expert in court cases. Eventually these activities were detected and Onubogu was arrested for these frauds and for indecently assaulting a 15 year old girl while examining her. He was jailed for five years.

While it is possible that the goal of these types of fraud is economically based, it could also be symptomatic of some form of mental illness or condition. In the case of Richmal Oates-Whitehead, there were a number of embellishments as to her medical qualifications. Miss Oates-Whitehead was found dead in 2005 due to a blood clot. Prior to her death Miss Oates-Whitehead had made news as one of the doctors praised for her work helping survivors of the Tavistock Square terrorist attack on July 7th 2005. Miss Oates-Whitehead claimed to be a doctor from New Zealand, but after her publicised activities on July 7th, the New Zealand press began to investigate her past and found she

had no qualifications as a doctor. At the time she was working as an editor for one of the publications of the British Medical Association, and she resigned from her post. According to the Sydney Morning Herald:

> "An investigation since Miss Oates-Whitehead's death has uncovered evidence that she led a fantasy life, telling others that she had travelled to Iraq to work as a doctor and to Indonesia to treat victims of the tsunami." (Sydney Morning Herald, 2005: 1)

Miss Oates-Whitehead also claimed to have been stalked, to have given birth to twins who had died, and to have been treated for cancer. She had also for a time referred to herself as 'Professor Richmal Oates-Whitehead'.

The practice of impersonating a general identity as opposed to a personal identity may not involve the persecution or victimisation of an individual who loses a part of their identity as is seen in cases of identity theft. Nevertheless as shown in the above incidents, people can feel that an abuse has taken place if they are dealing with someone who adopts a form of identification which they are not entitled to. There is also the abuse felt by people who have formed bonds of personal or social trust with the individuals who have lied about their membership of this social group.

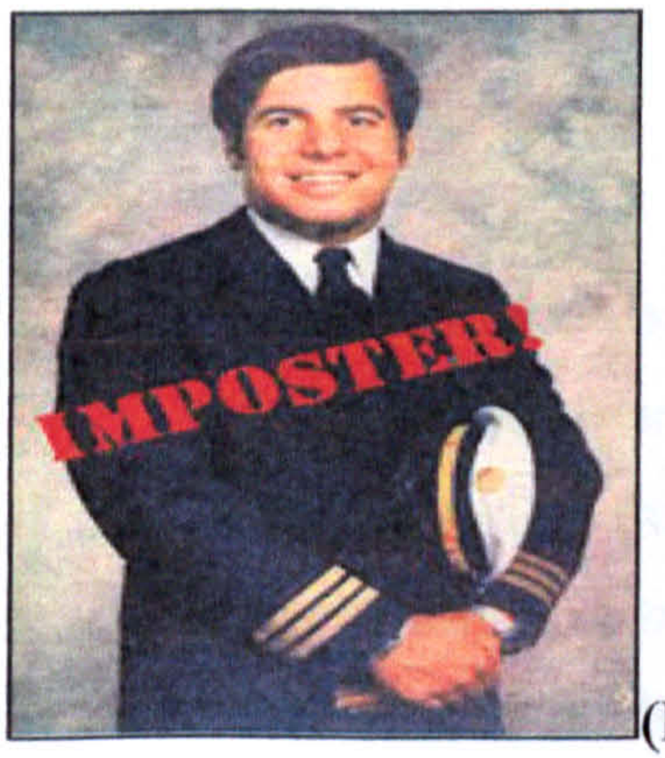
Frank Abagnale Jnr – airline pilot, doctor, lawyer

The one of the most famous 'con men' is Frank Abagnale Jnr. Abagnale performed a number of cheque frauds and falsified IDs in order to pretend to be a pilot for Pan Am, a doctor, a lawyer and a sociology professor in America in the 1960s. His story was used for the film called *'Catch Me If You Can'* (2002). Abagnale was able to cash over $2.5 million in forged cheques and was wanted in America and 26 other countries before reaching the age of 21.

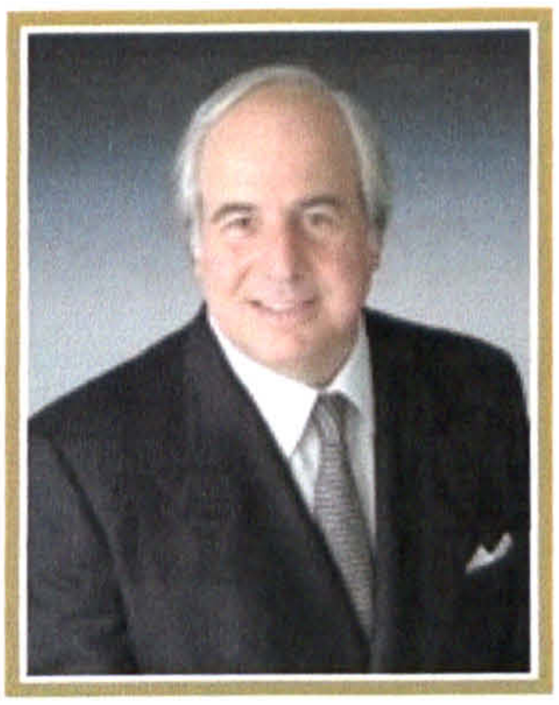
Rather than stealing the identities of others, Abagnale impersonated members of professions. Abagnale used various methods to convince people of the legitimacy of his

false identities, often using official looking documents which were enough to convince people that he was who he said he was. In the case of Abagnale's impersonation of a pilot, he was able to obtain an official Pan Am uniform simply by asking Pan Am where he could obtain a uniform.

His ability to do this in part was a product of the times. In the 1960s, the use of computer databases to make a note of 'who's who' did not exist. If someone said they belonged to a particular organisation (especially larger organisations such as Pan Am airways which was one of Abagnale's targets) the process of confirming this would be long and drawn out. According to Abagnale's own accounts, it would appear that as a consequence of this people were taken on their word, the quality and apparent authenticity of their paper proofs, and their ability to adhere to archetypes. When Abagnale he was eventually caught, he was wanted for prosecution in over twenty countries. However after spending time in French and Swedish prisons Abagnale was sent back to America to face prosecution. While Abagnale was imprisoned for a time in America he was eventually given an opportunity to work for the F.B.I as an expert in forged documents and the activities of fraudsters. Abagnale went on to start his own company in 1976, specialising in providing security for the banking industry and he now writes, and lectures on the subjects of forgery, embezzlement and secure documents to the F.B.I. academy, government agencies and corporations.



(Bell.R, 2008: 2)



Frank W. Abagnale
Author, Lecturer, Consultant (Abagnale and Associates, 2008: 1)

Identity fraud and deception as a means of attaining prohibited identities

While in many cases of identity fraud, the goal has been to defraud people, there are still some instances where people use identity fraud in order to obtain something they may be denied by society. It may be that in attempting to obtain this form of identification, they are breaking the law, but it may also mean that they are defying social norms and bonds of social trust. The following are several examples of people who have used identity fraud to obtain a form of identification that society, under normal circumstances, would deny them.

Miranda Stuart aka Doctor James Barry

An example which caused great controversy at the time was the case of Doctor James Barry, a celebrated surgeon and reformer of the British army medical service in the mid 1800s:

> "…The gentleman had entered the army in 1813, had passed, of course, through the grades of assistant surgeon and surgeon in various regiments, and had served as such in various quarters of the globe. His professional acquirements had procured for him promotion to the staff at the Cape. About 1840 he became promoted to be medical inspector, and was transferred to Malta. He proceeded from Malta to Corfu where he was quartered for many years… He there died about a month ago, and upon his death was discovered to be a woman. The

motives that occasioned and the time when commenced this singular deception are both shrouded in mystery. But thus it stands as an indisputable fact, that a woman was for 40 years an officer in the British service, and fought one duel and had sought many more, had pursued a legitimate medical education, and received a regular diploma, and had acquired almost a celebrity for skill as a surgical operator." (Manchester Guardian, 21 August 1865 cited in Lothene Experimental Archaeology 2007: 1)

According to Burton (2000), such was the concern over the case of Doctor Barry that some began to spread reports that, rather than being a woman, Doctor Barry was in fact a hermaphrodite.

Dr James Barry born Miranda Stuart (Levi Alter Website Computer Consulting Services, 2008: 2)

As well as the example of Dr James Barry, there are several instances of men and women who have lived their lives claiming to be the opposite sex. While today the term transgender may be applied to Dr James Barry and his lifestyle, in the 19th century the discovery that Barry was biologically a woman was scandalous. The use of deception with regard to gender is an area which arguably has become less criminal over time.

Archibald Stansfield Belaney aka Grey Owl

Another example of someone who has used identity fraud to obtain a form of identification that they would normally be prohibited is Archibald Stansfield Belaney. Belaney was an Englishman who in 1906 moved to Canada and adopted the persona of a Native American called Grey Owl. Belaney moved to Northern Ontario and married an Anishinaabe woman Angele Egwuna, he told her his father had been a Scot and his mother an Apache (in reality he was born in Hastings, England). In his life as Grey Owl, Belaney became one of the first environmentalists and conservationists and published several books under the name Grey Owl such as '*The Tree*' (1937) by Wa-Sha-Quon-asin (Grey Owl). Belaney's deception was discovered after his death and as a consequence his books were withdrawn from publication.

The activities of Belaney are an example of how it is possible for people to deceive others as to their ethnicity. A term associated with this activity is 'passing'. In America during the 20th century there were several cases of black people who 'passed' as white people. In Phillip Roth's book '*The Human Stain*' (2000), his main protagonist is a black classics professor who has passed for a white man for most of his life. According to Crary (2003) the story presented in *The Human Stain* is loosely based on the life of Anatole Broyard a literary critic for the New York Times. According to Crary:

> "Broyard was born to a black family in New Orleans and grew up in a black section of Brooklyn but as a young man stopped seeing relatives and friends from his past and lived the rest of life as white. A handful of people knew the truth, but even his own adult children were not among them." (Crary .D, 2003: 2)

Crary argues that this form of deception was in many instances a response to social inequality faced by black people in America.

Brian MacKinnon and Treva Throncberry - dcception and age

As well as identity fraud involving gender and ethnicity, people have also use identity fraud and deception with regard to their age. In 1993, Brian MacKinnon was a 30 year old Scot who enrolled in his former school Bearsden Academy in Glasgow Scotland as a 17 year old in an attempt to re-enter medical school.

MacKinnon adopted the persona of a 17 year old Canadian called Brandon Lee. MacKinnon created a back story for his new persona; he told the teachers that he was the son of William Lee, a Professor of zoology in Edmonton, Canada, and that his mother was an opera singer and that since his parents had separated he had been travelling with his mother and as a result had been privately tutored instead of attending regular schooling. MacKinnon went on to claim that his mother had died in a car crash earlier that year which had left his father severely injured and convalescing in Canada. MacKinnon's persona of Brandon Lee had been sent to Scotland to live with his grandmother. In a report for the Guardian, MacKinnon describes his experiences of going back to school:

"Waiting, shaking The best are faking and Christ, they were the opening lines from some old song, which came back to me repeatedly as I made my way through the open gates and down to the concrete yard. It was overcast morning in late May 1993, and I was 29 years old. The same old smells – state schoolyard mud squelched underfoot, followed by that peculiar 'school diner' aroma that pervaded a wide area around the canteen.

I was faced by the prospect of a year's drudgery, compounded by fear. Pausing at the entrance to the hallway, I tapped momentarily into the motivation that had brought me to this, to remind myself that I was doing the right thing; the only possible thing. " (MacKinnon .B, 1997: 1)

Despite his having attended the same school when he was a child MacKinnon's deception was working. The deputy head teacher accepted that Brandon Lee was a genuine 17 year old, and that he was at the Academy seeking for a year to gain

qualifications to apply for medical school. However when introduced to his fellow students it soon became apparent to them that MacKinnon was not a 17 year old. According to MacKinnon it was apathy on their part that saved him from immediate detection by the teachers. MacKinnon was able to enter Dundee University under the guise of Brandon Lee, but after a term he was unmasked; by this time he had dropped out because he lacked funds to carry on.

MacKinnon's story received a great deal of attention in the press and he has been denied access to any other medical school in the U.K. While this does constitute an instance of identity fraud, the goal was not criminal; in many reports MacKinnon has expressed a genuine belief that he is justified in seeking a career as a doctor. It is his obsession with becoming a doctor which has compelled him to seek the status through socially unacceptable means.

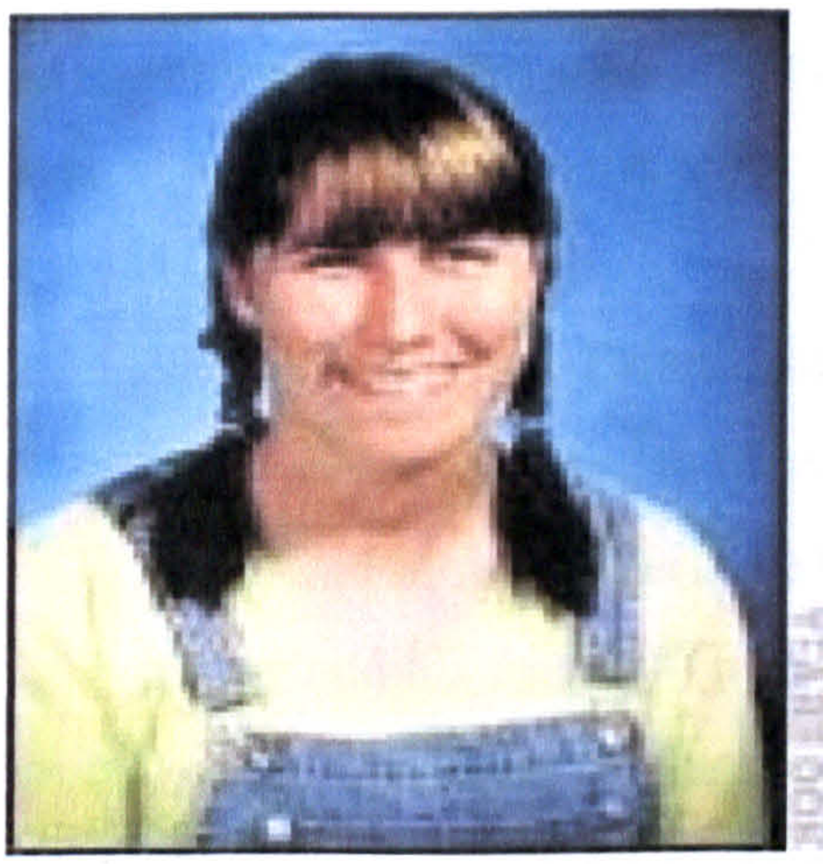
Another note worthy case of identity fraud and age is that of Treva Throneberry. In 2001, Throneberry was arrested for pretending to be a teenager when in reality she was (at the time of her arrest) a 31 year old woman who had been passing herself off as a teenager since the 1990s. While MacKinnon's actions can been seen as misguided, Throneberry's deceptions often involved not only criminal activity but also several damaging and untrue accusations. Throneberry's crimes included the use of false identities to defraud state foster care services and she was also charged over falsely accusing several people of raping her. She used several false identities and would routinely move to different parts of America and then claim to be a teenager from a broken family. She would gain access to social services and the local school system and pass herself off as a teenager in need of help.

According to Bell (2007), Treva Throneberry was born in 1969 in the state of Texas. As a young girl, it is alleged, she and her three sisters were sexually abused by an uncle. In 1985, Throneberry went to the police and accused her father of raping her at gunpoint. The charge was eventually dropped due to lack of evidence, but Treva was put into

foster care and placed with a family. She was moved to a new school where despite being a diligent student she would recount stories of horrific past experiences:

> "Treva started to tell stories of being kidnapped by Satanists, who tortured her by forcing her to watch them kill animals. The stories were never confirmed, were likely signs that she was experiencing delusional thoughts." (Bell .R, 2007a: 2)

Because of this story and claims she wanted to kill herself, Throneberry was sent to a State Hospital for psychiatric care. After spending five months in hospital she was sent to a home for troubled girls. At 18 she left the home and after a short time disappeared.



Treva Throneberry (Bell.R, 2006: 1)

In the subsequent years, Throneberry passed herself off as a teenager, using the aliases Keili Smitt, Cara Leanna Davis, Stephanie Lewis, Kara Williams, Emily Kharra Williams and finally Brianna Stewart. Throneberry used these identities in different states throughout the 1990s; she would go to a town and live in homeless shelters or in foster care eliciting help and support from people. In each instance, Throneberry told stories about how her father had been a Satan worshiping police officer who had raped her. Aside from accusing her father of sexual assault Throneberry also accused others of raping her; in 1993 she accused and pressed charges against a Portland Oregon police officer for raping her, claiming he was her father. Before the charges could be investigated, Throneberry fled from Oregon.

While in several instances Throneberry was able to enrol in local high schools passing herself off as a 16 or 18 year old, and enter foster care, there were occasions where her deceptions were discovered. In 1996, Throneberry's stories of being raped were investigated in Altoona Pennsylvania while Throneberry was using the alias Stephanie Lewis. This revealed her true identity and age (which at the time was 27) and resulted in a nine day prison sentence for filing a false police report. After this Throneberry disappeared again and moved to Vancouver Washington under the name of Brianna Stewart.

While using the name Brianna Stewart, Throneberry enrolled in yet another high school and re-entered the foster care system. Again Throneberry willingly recounted tales of physical and emotional harm:

> "Many who knew Brianna had some knowledge of her tragic life, something that she was not ashamed to hide. She claimed she had seen her mother brutally murdered by her father. She told stories of having been repeatedly raped by her father and his friends. Then at the age of 12, she purportedly ran away from home only to live on the streets and in countless foster homes, in different cities throughout the country." (Bell .R, 2007b: 1)

It was while living as Brianna Stewart that Throneberry's habit of making allegations about being assaulted brought her activities to light. Throneberry had made it clear that in the past she had been the victim of rape and in 1997 accused a man called Charles W. Bankenship of raping her. Bankenship was a 47 year old security guard who was charged with communicating with a minor for immoral purposes and sentenced to 365 days, 315 of which were suspended. Throughout the process of prosecuting Bankenship, no one discovered that Brianna Stewart aged 17 was in fact Treva Throneberry aged 28, and that Bankenship had been falsely prosecuted. After the prosecution of Bankenship, Throneberry moved between different foster families. One family suspected she was lying about her age; after a visit to a dentist suspicions were further raised by the dentist

who noted that Throneberry's wisdom teeth had been removed and the scars had healed much more than would be expected if Throneberry were 16, as she claimed. In 1999, Throneberry accused her latest foster parent David Gambetta, of spying on her with a camera while she was in her bedroom; the police investigation dismissed the allegations as there were a number of inaccuracies in Throneberry's story.

In 2000 after moving to live with another family, Throneberry's true identity was discovered and in March 2001 Throneberry was arrested. Throneberry was charged with several counts of theft and fraud, and the prosecution of Charles Bankenship was reopened. By pretending to be a teenager, Throneberry had been able to defraud the foster care system of $3,620.27 and obtained $1,050 of tuition from Clark College. She was also charged with perjury, obtaining false documentation and falsely accusing people of rape.

During the investigation into Throneberry's activities, D.N.A. tests and the dentist's reports were introduced as evidence; despite this Throneberry refused to acknowledge her true identity. She claimed it was a case of mistaken identity. The reasons for Throneberry's actions are hard to determine, but it has been suggested by lawyers and psychologists involved in the case that she suffers from a psychological condition which compels her to adopt new identities in this way and possibly that she believes the lies she is telling. Psychologists argued that if there were any genuine instances of abuse during Throneberry's childhood these could be potential cause for her actions. The prosecution argued that Throneberry was aware of her actions and even Throneberry herself denied the idea that she might have a psychological disorder, arguing that she was Brianna Stewart.

During the trial Throneberry elected to represent herself, but performed poorly, enabling the prosecution to easily win the case. Throneberry was sentenced to three years and two months on seven counts of fraud and perjury of which she served two years. After her release, Throneberry continued to claim she was Brianna Stewart and was able to obtain a driver's licence in that name. The licence also notes Stewart's age as 21.Unlike the

case of Brian MacKinnon who openly admits his deception, Throneberry is adamant in her claim that she is 21 not 31. While there were several incidents which put Throneberry's claims to the test, it is also worth noting that for ten years Throneberry's claims were at least partially successful.

Deception as a basis for criminal activity

Acts of identity fraud are instances that involve deception between individuals. It is possible to see in the history of identity related crime that criminals have been able to use identity fraud without using or needing to use identity theft. Giving the appearance of someone who can be trusted has been enough to enable crimes of deception. The value of a person's personal identity has been limited for many years by people's ability to communicate who they are over distance or for elements in society to confirm a person's claim to a personal identity.

In the examples discussed above, the personal aspects of an identity which an individual forms for themselves are not important. What is important is the adoption of social role and status which are elements of the identification process which individuals apply to other members of society.

The history of identity theft

It can be argued that before the advent of modern communication technology the identity of the majority of people was only known in their local community, the exception being people of higher classes such as the monarchy. It can also be argued that there was limited use for an individual's personal identity unless they were to some degree famous. Looking at historical accounts it is evident that there are several instances when people have attempted to adopt the identity of a monarch.

For example in 1598, Marco Tullio Catizzone failed in his attempt to pass himself off as King Sebastian of Portugal who had gone missing while on an expedition twenty years earlier. One of the major drawbacks of Catizzone's impersonation was his inability to

speak Portuguese and his identification as Catizzone by his wife whom he had abandoned.

Another later example of someone claiming to be a missing royal is the case of Anna Anderson who claimed to be Grand Duchess Anastasia in 1920. Anderson was a patient at a psychiatric hospital in Dalldorf Germany; she came to the hospital with no proof of identity or memory of who she was. It was only when people noticed her resemblance to one of Tsar Nicholas II's daughters, the Grand Duchess Anastasia, that questions over the true identity of Anderson were asked. There was a great deal of speculation that Anastasia had avoided the executions of her family. The idea that Anderson was Anastasia led to a number of Romanov family members supporting her claims to the Russian throne. However, as with the case of Catizzone and his impersonation of King Sebastian, Anderson's impersonation had a major flaw: she could not speak Russian. Like Catizzone she attempted to explain this discrepancy, according to Burton (2000):

> "The pro-Anderson lobby must have been moved by powerful motives indeed to accept a Russian princess who spoke no Russian. Anderson explained many years later in her 'memoirs' that it was not that she could not speak Russian but, just as she did not like to talk about events surrounding her escape {because 'I had suffered such awful things that I did not want to be reminded of it'}, she likewise 'had also decided always to speak German, because Russian had become disagreeable to me'." (Burton .S, 2000: 107)

Accounts of people who pretend to be lost or dead royals often involve the inclusion of people who will corroborate the impersonator's claims, regardless of how credible they are. It can be argued that they do this because there is a possibility they will gain access to power or wealth through the impersonator. Also since these impersonations can involve a political element, there is the risk of being considered treasonous for having doubts or being sceptical.

One of the most famous cases of identity theft is that of the Tichborne Claimant. This case involved a man called Arthur Orton whose prolonged attempt to claim the identity of Roger Charles Doughty Tichborne became a highly publicised case in the 19th century. Sir Roger Charles Doughty Tichborne was the heir to the Tichborne estate who 1854 was travelling back home to England from Rio de Janeiro. His ship was lost at sea with all hands, and after a year Sir Roger was pronounced dead and his title and estates were transferred to his younger brother.

Roger Tichborne (left) and Arthur Orton

(Orton.P, 2008: 2)

Despite the pronouncement of Sir Roger's death, his mother refused to believe that her son was dead. She sent inquiries all over the globe looking for any sign of him and in 1865 she received word from a lawyer based in Sydney who told her that a man fitting the description of her son was living in Wagga Wagga Australia. In reality, the man was Arthur Orton, a butcher, who despite bearing a slight similarity to Sir Roger was not the real Sir Roger Charles Doughty Tichborne. Aside from some vague similarity in facial features there were more reasons to believe that Arthur Orton was not Sir Roger. In appearance Sir Roger had sharp features and black hair while Orton's features were rounded (he was quite fat) and his hair was light brown, and most crucially, while the real Sir Roger had been raised in France as a child until the age of 16 and could speak fluent French, Orton could not speak a word of French.

Despite this Lady Tichborne deluded herself into believing Orton was her son. Lady Tichborne sent money to Orton to come and see her. When Orton was finally exposed he explained the reasons for accepting and continuing the deception:

> "The reason I wrote the letter (to the dowager Lady Tichborne) was because I was hard pressed for money at the time, and I thought that if she was fool enough to send me money so much the better. I could go to Sydney and take the steamer to Panama where I could join my brother, and nobody would ever hear anything from me. I learned about the Tichborne family in Burke's Peerage, which I saw in Goulburn, and enabled me to converse about different members of the family.
>
> Bogle thoroughly believed I was Sir Roger, he used to converse very freely with me about the family, giving me the whole history of it ... I was pumping him all the time as to names and habits and customs of various members of the family. I have always been a good listener and by listening quietly and patiently for hours, to statements which have been made to me by, I suppose, I may say hundreds of people, all of whom gave information concerning the Tichborne family. I learned such facts that really induced me to prosecute my claim. I found by listening to others the story built itself and grew so large I really couldn't get out of it.
>
> I could not get away from those who were infatuated with me and firmly believed I was the Real Sir Roger ... Of course I knew perfectly well I was not, but they made so much of me, and persisted in addressing me as Sir Roger, that I forgot who I was and by degree I began to believe I really was the rightful owner of the estates. If it had not been that I was feted and made so much of by the colonialists in Sydney I should have taken the boat and gone the rest of my days to Panama with my brother." (Arthur Orton, 1895 cited in Sniggle.net, 2007: 18)

While it was Orton who perpetrated the impersonation he did have help from a number of supporters. The first of these was Andrew Bogle, an old friend of Sir Roger's father; there were also the Tichborne family solicitors, Edward Hopkins and Francis J.Baigent, who met with Orton when he made the trip to London in 1866. In January 1867, Orton went to Paris to met Lady Tichborne, who immediately identified Orton as her son. After the meeting, Orton was given an allowance of £1,000 a year. As Orton says (see above), he then encountered several others from whom he derived information to improve the impersonation.

The case of the Tichborne Claimant illustrates how even the most implausible impersonations can be achieved if the people who are being deceived are eager to accept the information with which they are presented. However, Orton's deception was revealed eventually by those who were not so eager to accept Orton's story. Other members of the Tichborne family investigated Orton and found that while he was in England staking his claim to the Tichborne estate, he had enquired about his real family who were living in Wapping. Orton's claim was also put under further pressure when his main supporter Lady Tichborne, died in 1868. While Orton could have ended his deception then and escaped, he had by this time raised significant debts in his claim to the Tichborne estate. The story culminated in a trial at the Court of Common Pleas in May 1871. The trial involved examinations of the discrepancies in Orton's accounts and his inability to speak French, despite presumably spending his youth in France, and Orton's brother was brought into deny the claim the Orton was Sir Roger. In response, over a 100 people were brought into confirm that Orton was Sir Roger. Ultimately, the jury decided against Orton, denying his claim.

After the trial Orton was charged and convicted on two counts of perjury and was sentenced to 14 years hard labour, of which he served 10. Orton died penniless in 1898. The case of the Tichborne claimant can be seen as an early and elaborate form of deceased identity fraud. In modern instances of this type of identity fraud thieves attempt to steal pensions from the recently deceased elderly, or they claim state benefits that the deceased would be entitled to if they were still alive; in the Tichborne case

Orton went one step further and attempted to acquire Sir Roger's inheritance, status and social network of friends and family members.

In the above examples, there is variation in the ability of the individuals involved to impersonate the individuals they claimed to be. However, they do in many respects highlight several elements of identity fraud which would later become staple aspects of modern identity fraud. The targeting of a specific individual and the accruing of supporting evidence and in particular, as in the case of Orton, the adoption of additional information from third parties, are all aspects of modern identity theft. It can be argued that what has changed has been the willingness of criminals to target a more diverse range of people.

F.W.Demara – the Great Impostor

One man who has used both the theft of archetypal identities and the theft of specific people's identities is F.W.Demara also known as the 'Great Impostor'. Demara's activities were immortalised in the 1960s film 'The Great Impostor' and several reports in Life magazine documenting his activities. What is interesting about the case of Demara is that his impersonations were intended to enable access to professions rather than be a means of defrauding the legitimate identity holder or the organisation Demara worked for. Ironically, he was a great success in the numerous professions he worked in, despite gaining access to them through deception. Demara is also an example of a con artist who utilised both identity fraud against individuals and identity fraud against more general forms of identity.

In a career that spanned three decades, Demara impersonated several people including a doctor in the Canadian Navy and passed himself off as an academic, prison warden and a monk. According to Burton (2000), Demara had several aliases: Dr Robert Linton French, Dr Cecil Boyce Hamann, Dr Joseph Cyr, Jefferson Baird Thorne, Martin Godgart, Ben W.Jones and Anthony Ingolia. Demara utilised both the theft of an individual's identity and the impersonation of archetypal or general identity.

F.W.Demara – The Great Impostor (Peate.L, 2008: 1)

Demara spent most of his life using false identities and lying about who he was. He was born in 1921 in Lawrence Massachusetts and at an early age had an interest in joining the Catholic Church. At fourteen he ran away from home and tried to join a Trappist order in Rhode Island, where his parents reluctantly allowed him to stay believing that the strict life of a monk would soon prove to difficult for their son. Demara stayed at the monastery for two years and earned his hood and habit, being given the title Frater Mary Jerome. However the monks at the monastery felt Demara lacked the right temperament to be a monk. Forced to leave the monastery, Demara then attempted and failed to join two other monastic orders. His efforts to become a priest ended when he stole a car from the Brothers of Charity children's home in West Newbury.

Demara moved on and joined the U.S. Army, a decision he soon regretted. He sought a way out of the army and found it in the identity of his friend Anthony Ingolia. The two were stationed at Kessler Field Air Force base in Biloxi Mississippi. One weekend Ingolia decide to take his friend home with him, when they arrived Ingolia mother spent some time explaining to Demara details of her son's life. While these details seemed harmless to Ingolia and his mother they would prove invaluable to Demara. He used the information to steal Ingolia's identity, according to Robert Crichton (1959), Demara's biographer:

> "Since his aim was to do good, anything he did to do it was justified. With Demara the end always justifies the means. Stealing Ingolia's papers was not in itself a bad act if he didn't do bad things with them. It was, in fact, a good act." (Crichton 1959, cited in Burton .S, 2000: 75)

After stealing Ingolia's identity, Demara left the Army and after a couple of years joined the U.S. Navy under his own name. In the navy, he sought to be accepted to medical training course and while he proved adept at the basic courses, he was denied access to advanced training because he lacked the correct educational qualifications. In order to get around this, Demara began fake and forge documentation to gain access to the medical school; he was so impressed with his attempts that he bypassed trying to go to medical school and went on to try and gain a commission as an officer. His hubris cost him however, as his efforts were detected. Demara was aware that eventually he would be arrested for his actions, so he faked his death by putting a naval uniform and a suicide note on a quayside.

After faking his death, Demara faked his identity again. He became Dr Robert Linton French, a former naval officer and a psychologist. Demara worked at several churches around America as Dr Linton and this culminated in his establishing a school of philosophy and teaching on the subject of psychology at Gannon College in Eerie, Pennsylvania. While Demara proved to be a highly competent teacher, suspicions began to arise amongst staff at the University. Demara's career at Gannon came to an end when the Navy found him out and arrested him for desertion. Demara was charged and sentenced to six years in prison. He served eighteen months of his sentence and was released because of good behaviour. According to Burton (2000) Demara disliked the status of being an ex-con:

> "As Dr French, those cops wouldn't have treated me that way. I really hated not being French. No. What I hated most was being Demara again. Who was Demara? Anyway you looked at it, French was somebody, good or bad. Good or bad, Demara – that guy was a bum." (Burton .S, 2000: 82)

In response to his dissatisfaction with his status in society, Demara began impersonating and inventing identities again. He enrolled in Northern Eastern University as Cecil Boyce Hamann and attempted to complete a degree in Law. He soon lost interest and instead of gaining a qualification simply claimed to have a PhD. Dr Hamann as Demara would refer to himself, as was a zoologist. He went to another Christian institution in Maine – the Brothers of Instruction - and took up a teaching post; and it was here that he met Dr Joseph Cyr. Cyr's identity would prove to be one of the most noteworthy of Demara's impersonations. Cyr had moved to America from Canada and was a doctor seeking a licence to practice medicine in America. Demara became friends with Cyr and offered to help him in his efforts to gain accreditation. Demara took (although he claims they were freely given) all of Cyr's documents under the pretence of helping Cyr. Eventually, Demara left his job with the Brothers of Instruction and moved north to Canada. At this time, the Korean War was causing {amongst other things} a distinct shortage in the number of doctors available to the Canadian military. Presenting Cyr's credentials to the Canadian Navy in 1951, Demara demanded a post as an officer saying that he would otherwise join the Canadian Army. In response to this ultimatum, the Canadian Navy rushed the acceptance process for Demara, and within days Demara had become a Surgeon Lieutenant in the Royal Canadian Navy.

Demara was posted to RCN Stadacona hospital in Halifax and then to the HMCS Cayuga a ship sent to patrol the waters off the east coast of Korea. This meant that Demara was now responsible for the well-being of a crew of 292.While he was aboard the Cayuga, Demara's impersonation was put to the test when the ship picked up three injured South Koreans who had been involved in guerrilla fighting. Demara had to operate and successfully removed a bullet from the chest of one man and amputated the foot of another. All his patients survived and his work earned him the respect of the crew and a great deal of attention. Many of officers of the Cayuga wanted to put Demara forward for a medal. It was this attention which brought about an end to Demara's impersonation.

News of Demara's activity had been picked up in the news papers, and one of the people who had read of his exploits was the real Dr Cyr's mother. While Demara was posing as Cyr on the Cayuga the real Dr Cyr was practising medicine in Grand Falls, New Brunswick. Cyr found that while it was his name in the paper, the picture was of his friend Dr Hemann from Maine. Upon discovery that Demara was an impostor a message was sent to Captain James Plomer of the Cayuga in October f 1951:

> "Captain's eyes only, have reason to believe your Medical Officer is impostor. Investigate and report." (Sugrue .C, 2007: 1)

Further investigation and a search of Demara's room revealed letters and documents that proved he was not Dr Cyr. Demara was transferred to a British ship and sent back to Canada. Demara's exploits as Dr Cyr were eventually made into the film '*The Great Impostor*' in 1960 with Tony Curtis taking the lead as Demara.

How Demara was able to pass himself off as Cyr for so long is due in part to the character of the man. Demara, while critical of those who sought education, had a good memory for facts and was able to learn very quickly. Demara also manipulated others to aid him in his deceptions. While at Stadacona naval hospital he had approached one of his superiors asking for their help in putting together a booklet which would act as a rule of thumb guide on medical matters. Demara claimed the guide was meant as help for lumberjacks who were often very far from immediate medical assistance. Demara would use this quick guide, as well as lessons he had learned from previous work he had conducted in a hospital in Los Angeles. Onboard the Cayuga, Demara also had the help of a competent sick berth attendant who handled most of the minor cases. In fact this attendant Petty Officer Bob Horchin, was pleased to have a superior who did not interfere in his work.

After returning to America Demara moved on with his career as an impostor and found himself using the identity of Ben W. Jones. With this identity, Demara began work at Huntsville Prison in Texas as a prison guard. As with many of the professions Demara

attempted, he was a success, gaining the admiration and respect of the governor and prisoners. Demara was eventually put in charge of the maximum security wing which housed the most dangerous prisoners. For a while, Demara was content and appreciated; however the attention his activities had received by the media proved the downfall of his efforts to be Ben W. Jones. A report by Joe McCarthy for Life magazine in 1951 on Demara's exploits resulted in Demara's detection as Jones.

Again, as with the incident in Canada Demara was detained, but again as with Canada, the state of Texas did not prosecute Demara for his deception. In 1959 Robert Crichton wrote about Demara and his exploits; below is an extract from his book:

> "His arms swung from side to side and this, combined with his bulk, gave him the appearance of a graceful bear.
>
> When he saw the detectives, a look of surprised hurt crossed his face and he stopped exactly as suddenly as if he had been shot. For a moment he seemed to teeter where be stood, unsure of whether he was going to fall forward or tip backward, then he finally came on ahead.
>
> "I have a feeling I can be of help to you two men," he said softly. "What took you so long to get here?"
>
> "Let's do it this way first," Nickerson said, flourishing a paper, a warrant for Godgart's arrest, in his hand. "You are Martin Godgart?"
>
> "In a manner of speaking, yes," the big man said.
>
> "Your real name is Ferdinand Waldo Demara, Jr., is that right?"
>
> "Sometimes it's hard to say what my name is."
>
> "Let's do this thing right," Milligan said. "This is an arrest."

"All right, then. I was born under that name but I use Fred W. Demara now." Nickerson was checking against a small notebook.

"Alias Martin Godgart?" he asked. The man nodded yes. "Alias Dr. Robert Linton French?" There was another nod of yes.

The detective studied the list for what seemed a long time.

"My," he said, "that Dr. French really got around. You went places with him."

"I did. He was one of my best," the teacher agreed. "Alias Brother John Payne?"

"Alias Dr. Cecil Boyce Harmann?"

"You people have been doing your homework. Yes, I was him too."

"Alias Ben W. Jones, assistant warden of the Huntsville Prison in Texas?"

I'm not ashamed of that one."

"Alias Dr. Joseph C. Cyr, surgeon lieutenant in the Royal Canadian Navy?"

"One of my very best," the prisoner said. He saw that Nickerson was closing his notebook. "Go ahead, go ahead. 'You've missed some."

(Crichton .R, 1959: 2-3)

Demara eventually became a clergyman under his own name and died in 1981. The activities of Demara are in many ways unique and cannot be seen as a typical example of an identity thief. But the manner in which he gathered and used information about

people, and his manipulation of organisations are informative in displaying the lengths to which someone can use deception and impersonation.

The art of impersonation

The examples of early incidents of identity theft presented here outline how for the most part early identity thieves sought out the advantages found in the lifestyles of the people they impersonated. For Catizzone, Andersen, Orton and Demara it was the social status, role and resources (property and/or money) of the people they impersonated that they wanted. This meant a high level of commitment to the impersonation both in terms of their time and personal well-being.

It is argued in this study that as communication technology has improved people's ability to communicate their identity over larger distances in shorter amounts of time, the need to commit to the impersonation in the way the early identity thieves did has decreased. While there are exceptions, such as the case of Charles Stopford, modern identity thieves do not have to commit to their impersonation to the same degree. Also the focus of modern identity theft has shifted to obtaining the resources associated with a personal identity. Early examples of identity theft were prolonged acts of impersonation; modern identity theft is quicker and in some respects easier to commit. This has resulted in the use of identity theft becoming a more viable option for those seeking to commit identity fraud – acts of misrepresentation.

The modern view of identity fraud and identity theft

While it has been argued in this chapter that the history of both identity fraud and identity theft can be tracked back several centuries, the use of the terms identity fraud and identity theft is a modern phenomenon. Due to media representations of identity fraud and identity theft, a misconception has developed that these are new crimes.

In the U.K. the 'new crime' of identity fraud was introduced to the general public through the experiences of Derek Bond. Bond's imprisonment in South Africa in 2003 came about at a time when concerns over the identification process were at a high with

concern over terrorism and illegal immigration (see case of Derek Bond page 113). The terrorist attacks in America in 2001 resulted in a rise in concern over the identification of terrorist threats. Concern with regard to terrorism was also raised with the 2004 bombing in Madrid, the terrorist attack on London in 2005 and the 2007 car bombing of Glasgow airport.

In 2004, the deaths of 23 Chinese illegal immigrants in Morecambe Bay raised concern over illegal immigration, and the identification of illegal immigrants in the U.K. The common theme connecting these areas of criminal activity is the issue of securing the identification process. As a result of this, the issue of securing the identification process has been raised and put at the forefront of crime prevention efforts. New anti terrorism laws, and the proposed introduction of an identity card scheme, have attempted to address this raised level of concern. As well as the experiences of Bond in 2003, the discovery of Charles Stopford's 23 year deception in 2005, and connections made between identity fraud and the internet, have further raised the profile of identity related crime in the 21st century.

The reason identity theft and identity fraud have become such major concerns in the 21st century is that now more than ever there is value to a person's personal identity. Consequently, those who would have been satisfied in previous centuries with acts of misrepresentation (identity fraud) and fraudulent deception, are now in the 21st century using impersonation (identity theft) to greater degree than ever before. By using stolen identities, fraudsters can make money, enter the country illegally or enable terrorist attacks.

Conclusion

The history of identity related crime has shown an ever strengthening link between the use of identity theft and identity fraud. The ability to use and obtain information about individuals has expanded and developed the use of identity fraud. Whereas in previous centuries people like William Thompson and Frank Abagnale Jnr could use deception and subterfuge to commit identity fraud, the abundance of information available about

people's personal identities and the venues where this information can be used means identity theft is a far easier means of enabling identity fraud. The terms identity theft and identity fraud can be seen as recent developments but the activities they describe are well established forms of criminal activity. The use of misrepresentation in early cases of identity fraud shows how criminal activity has capitalized on the inability to reliably confirm identities.

By differentiating between acts of impersonation and deception, it is possible to see how over time the value of a person's personal identity has increased. Early examples of identity theft have been aimed at people whose identities have been communicated over a wide area, such as in cases where people have impersonated royalty. As technology has improved, it has become more viable to abuse personal identities; this can be seen by the rise in the instances of identity theft.

Identity fraud and identity theft are not new crimes, but thanks to developments in technology and identification processes, the number of people susceptible to these types of crimes has increased significantly. It can be argued that the use of the terms identity theft and identity fraud illustrate this development as it has become necessary to inform and protect more people from this type of crime.

In the next two chapters there is an outline of how modern identity theft and identity fraud are committed; this outline is presented in the form of a progression. This progression shows how identity theft and identity fraud have become more interconnected in modern cases of identity related crime.

CHAPTER 7

Gathering and Appropriating Information on Identities

The process of defining identity theft and identity fraud is something that a number of experts in the area of identity related crime have endeavoured to do. However there are often vast differences in the specifics of what constitutes identity crimes. These differences can involve terminology but also the scope of the crime. As discussed in chapter 6 it is necessary to distinguish between forms of identity theft which rely on stealing a personal identity and identity fraud which relies on deceiving an organisation or other individuals.

Identity theft – The impersonation of a specific person's personal identity. This victimises the individual and their presentation of self. The act of identity theft can and often does lead to a further instance of identity fraud. The emphasis here is to impersonate a person's personal identity and benefit from victimising that person.

Identity fraud – Deception, either through the use of a false or stolen identity victimising society and their trust in a person's social role and/or social status. The emphasis here is on abusing individuals in society by deceiving them as to who the identity fraudster is.

As discussed in chapter 6 the crimes of identity theft and identity fraud have become more interconnected in recent years. In the light of this, the modern practice of using identity theft to enable identity fraud is discussed, rather than treating the two crimes as separate entities.

Previous definitions and the input of others

When attempting to classify or define identity related crime, the usual approaches are to use either the term identity fraud or the term identity theft, or to use both terms to describe different aspects of the same subject.

For example, the definitions used by Finch (2003) discuss identity related crime in terms of partial and total identity theft, whereas Semmens (2005) refers to identity theft as a long term offence, where a person's identity is appropriated entirely and to identity fraud as a short term offence against someone's identity, usually for the purpose of stealing funds or resources. These definitions and the definitions of others discussed in chapter 3 are useful for providing a broad idea of what identity theft and identity fraud are. These definitions, however, do not provide a detailed explanation of how identity theft and identity fraud are committed. The goal in presenting this progression is to provide a more comprehensive view of how these crimes are committed, in order to better understand what impact a National Identity Card Scheme would have on them.

When attempting to establish this progression, a wider array of terms were needed, and as mentioned earlier, the first two terms that were used were identity theft and identity fraud. Other terms were necessary, and initially terms such as fake and false identity were used. These were terms that had been used in the past to describe identity related crimes. However, these terms could not describe the type of activity that takes place when someone attempts to commit identity fraud. What was needed was terms that could explain the different ways an identity can be manipulated or misused.

The first terms that which were considered for use were the concepts of appropriation and impersonation discussed by Semmens (2005). Using the terms impersonation and appropriation, it, became possible to develop more terms that could explain the different stages of the identity fraud progression.

The terms gathering and appropriating are used to refer to gaining information; impersonation and misrepresentation are terms used to explain the difference between identity theft and identity fraud. For the final stage - the identity fraud itself - categories developed by the Fraud Advisory Panel (2003) account takeover, false application and wholesale assumption. Also included is the term breaching security, to describe the acquiring of identifying details that do not immediately have any financial benefit or are

intended as a means of accruing identification as a means of enabling more complex identity fraud or as a means of circumventing a security system. Also, the term partial assumption is used to describe situations where people have two or more identities that they use at the same time.

A U.K. view of identity theft and identity fraud

By developing this progression, it will be possible to understand how a person's identity is stolen in the U.K. The use of work from other countries has been included in the progression, for example the work of Newman and McNally (2005) on identity theft in America. The definitions developed by Newman and McNally draw on the reasons people commit identity theft and identity fraud in America: for financial gain, to hide a criminal past, and to establish a new life. These reasons are included in this progression as they appear to be universal motivators for this type of crime.

However, the work by Newman and McNally is based on the American experience of identity related crime. There are a number of significant differences between the U.K's experience of identity related crime and the U.S. experience. Firstly, there is a huge difference in the way the identification process is operated in the U.S.A. which has different proofs of identity and different systems of protection and security surrounding various forms of identity. Secondly, America has established the crime of identity theft as an indictable offence, making it easier for prosecutors to explain and define the actions of people who commit identity theft. In the U.K., the legislation introducing the National Identity Card Scheme expands on previous legislation to make the use of 'false representations' a crime. Until this law is introduced, identity related crime is only investigated through the various abuses of the identification process, such as providing false information on an official document (see case of Charles Stopford 115). Thirdly, there is a difference in the approach to solving the problem of identity related crime. The U.S.A. has rejected the use of ID cards, but does have a driver's licence which includes a photo and acts as a de facto ID card. In the U.K., the main approach to dealing with ID crime is the introduction of an ID card. Other differences include the focus on particular reasons for committing identity fraud. In the U.K. abuse of the welfare state is a bigger

concern as there are a number of services such as free healthcare, unemployment benefits and state pensions. Abuse of similar services in the U.S.A. is more likely to be covered under the abuse of private organisations.

Another area in which Britain and the U.S.A differ in their experiences of identity theft is in the publicising of the crime. In the U.S., the victimising of people by identity thieves has been well documented since the 1990s through the work of groups such as the Privacy Rights Clearing House, Identity Theft Resource Centre and the Knightsbridge Castle Group before identity theft became a big issue in the U.K. In the U.K., only 2% of victims directed towards victims support services are victims of fraud. Of this percentage, there is no distinction between the different types of fraud. While instances of identity theft have been reported in the media, there is still no victim support system designed to help victims of identity fraud. In the U.S., there are several groups who cater to victims of identity fraud, for example the Privacy Rights Clearing House, the Identity Theft Resource Centre and the Knights Bridge Castle Group. While the threat of identity fraud has received increased attention in the U.K., there has been less attention given to victims of identity fraud.

Geography also plays an important role in defining identity related crime for the U.K. As America is a collection of states, there are more communication concerns with regard to verifying identities. Illegal immigration and the role of organised crime groups is a major concern. It has been reported that the major threats to the U.K. from people smugglers come from eastern European gangs.

While work from America and Australia has been reviewed in earlier chapters, it is important that the progression presented here represents identity fraud in the U.K. specifically. This progression is an attempt to show identity fraud in the U.K. – what is stolen, why, and how. Before outlining the different methods of gathering and appropriating information on people, the identification process will be discussed.

Identification process

The approach to the identification process used here is based on observation of identification processes used by individuals, government agencies and private organisations. When attempting to identify someone there is a dual process enacted, where society or a group within society, seeks to identify an individual, and an individual seeking to be identified puts him or her self forward to be identified. The identification process is something that both society and individuals engage in. The process displayed here is society's efforts to identify individuals; there is equally a process by which individuals try to identify themselves to society.

When society seeks to identify someone, they are searching for several different factors. These factors can vary in terms of their importance but they are all present in the identification process. The first is safety; part of any identification process is determining that there is no threat of harm, either physical or more abstract forms of damage. For example, when a bank considers an applicant for a loan, part of the identification process is to determine if that person can be trusted. Establishing whether or not a person is dangerous has been fundamental to the identification process for centuries: for example, early on, gestures such as shaking hands developed as a means of showing that a person does not have a weapon in their hand.

Physical appearance and biometrics have always played an important part in the identification process; not only do we establish a person's trustworthiness by what others look like and our own understanding and preconceptions of the meaning of their appearance, but physical appearance also plays a part in confirming identity. The use of physical appearance and biometrics in the identification process has diminished somewhat with the advent of systems of long range communication such as the mail service and telecommunications technology such as the phone and the internet. Returning an identity to a specific person is truly the only way of confirming who someone is.

The next element of the identification process is the establishing of social status and role, which is where previously established forms of identification come into play. The fourth element of the identification process is the establishment of eligibility. Individuals seek identification by society and other individuals for a reason, often to seek access to some type of service or inclusion in a social group. As mentioned earlier, there is also an identification process within which individuals attempt to identify themselves to society. Here the key issue is what the individual desires society's to acknowledge about them. Identity fraud can be seen as an attempt to control both societies' efforts to identify the individual and how the individual's identity is acknowledged by society. The distinction between society's identification process and the individual's identification process can be seen as the first distinction between types of identity fraud. Frauds that involve manipulating society's efforts to identify the individual can be seen as the more short term frauds such as credit fraud. These frauds do not require that society acknowledges that the individual is genuine in their identity, only that they be allowed access to society because of it. Longer term identity fraud such as assuming a new identity for life (wholesale assumption) requires that certain parts of their identity (namely the new name) be acknowledged by society, which places these types of fraud more in the sphere of the individual's efforts to identify themselves. The simple distinction would relate to how much of the fraudster's efforts and success are reliant on society seeing them as someone other than who they are, and the duration of the impersonation.

While there are numerous ways to change identity illegally, it is not a crime to use another name to the one displayed on a birth certificate. It can be argued that identity is a declaration of who an individual is, and as such this is open to change at any moment. When people are identified in terms of their emotional state, the identification process is reliant on change in a person's appearance to note a change in their mood to identify when they are happy and when they are sad. Other forms of identification, such as identifying someone according to their age are reliant on there being a difference in how a person can be identified over time.

Change in identity is natural and necessary, but there is one area in which change in identity is less common or accepted and that is in a person's name. While our identity can change through time, it is necessary for at least one part to remain the constant in order to accurately track an identity. If a physical form could be kept from aging or changing its appearance then it could be used as constant identifier. It can be argued that D.N.A. is the only truly constant identifier, however, the use of D.N.A. in identification processes is limited at present.

Types of identifying document

In the U.K., there are several types of identifying document. These allow citizens access to resources such as accommodation, state welfare and the credit industry, and these documents are also used to prove identity. Below is a list of several different types of identification that are commonly used in the U.K. to prove identity.

- valid passport
- standard acknowledgement letter (SAL) issued by home office (HO)
- Application Registration Card (ARC) issued by Home Office (HO)
- identity card issued by European Union (EU)/European Economic Area (EEA) member state
- Form GV3. A one way travel document issued by United Kingdom (U.K.) embassies abroad
- U.K. residence permit
- full driving licence
- local authority rent book/card
- council tax documents
- life assurance/insurance policies
- mortgage repayment documents
- recently paid fuel/telephone bills in customer's name
- original marriage certificate
- original birth/adoption certificates
- divorce annulment papers

- certificate of employment in Her Majesty's Forces
- certificate of employment under the crown
- certificate of employment in the merchant navy
- wage slip from recent employer
- trade Union (TU) membership card
- travel pass with photograph affixed
- vehicle registration/motor insurance documents
- expired passport
- Form B79 – a form used to notify Department for Works and Pensions (DWP) staff that a person has been discharged from prison and has been advised to claim benefit

Cheque books, cheque guarantee cards and store/credit cards are also used to prove identity. A National Insurance Number Card (NINO) on its own is not evidence of identity but it can be used in conjunction with other documents. Often people who are required to confirm identity use a selection of questions and requests for information to confirm and corroborate claims of identity. Below are examples of questions used by the Department for Works and Pensions:

- Surname/family name, ask if there are other ways of spelling the name
- Forenames or first names
- Previous names
- Date of birth
- Current address
- Previous address
- Any other names/alias or known as
- Dependant details
- Employment history
- Name and address of previous employers
- If person from abroad – details and dates of arrival in U.K?

- Type of benefit claimed – does this match information provided by customer?
- How much benefit was in payment?
- Which Post office was used to collect benefit
- Bank details

Often the provision of identification documents is spaced over time, as eligibility can be dependant on age or financial status. Eligibility for identification is also dependant to a degree on society's opinions about when an individual is mature enough to be given responsibility for certain forms of identification such as being allowed to drive a car. Below is a guide as to when certain types of identification are issued or can be applied for. This breakdown of when identification becomes available is important as time and age of the identity thief can affect the difficulty faced when trying to steal or appropriate a particular type of identification.

At birth

- Parental notification to hospital/mid-wife of newborn's name and then information is given to the registry office by parents and hospital. Then an 'Entry from the Register of Births' is given (birth certificate, has unique number).
- National Health Service Preliminary Medical Card
- National Health Service Number
- Exceptions- Adoption and Immigration

Young adulthood

- National Insurance Number- issued before 16th birthday
- Provisional/Full Drivers Licence

Adulthood (18-60)

- Passport
- Mortgage
- Insurance
- Bank Account

- Credit Cards

Old Age (60+)

- Pension Allowance
- Disability notification

While the question of what is an identity and what should be included or excluded in defining an identity is still open to debate in academic study, processes of identification carry on regardless; it can be argued that a person's identity is whatever is used to prove eligibility for various services available to members of society.

Gathering and appropriating

The first stage of this progression is an information gathering stage. In her definition of identity fraud and identity theft, Semmens (2005) refers to this stage as appropriation. Semmens also refers to impersonation as a part of identity related crime. These terms were used within the progression as they help to distinguish various parts of identity crime.

While the use of terms such as identity fraud and identity theft describe what is done with an identity, they fail to describe the activities that take place. Describing something as fraud or theft does not explain what happens to the identity during the process of impersonation or the use of deception. Theft and fraud are very much the end results of a corruption of the identification process. They fail to describe how a person's identity is transformed through the input of an illegitimate user.

Identity related crime

In this study, identity related crime is broken down into a progression with three stages of activity. The first stage in this progression is the gathering and appropriating stage. Gathering refers to the legal forms of identifying information, and appropriation is the illegal approach to information gathering. This distinction is used because the gathering and appropriating of identifying information about other people can be done both legally and illegally. The forms of gathering information described in the progression represent

the types of information available and the methods of obtaining it. The illegal methods of obtaining an identity involve intercepting information and communication going to and from the legitimate identity holder. Also, previous successful attempts at stealing a person's identity can be used to further corrupt a person's identity. Third parties can also be used to enable gathering and appropriating, as is seen when corrupt employees steal information from their employer.

Legal forms of gathering and appropriating

While illegal methods of obtaining information about a person's identity have received a lot of attention, information can be obtained through legally permissible means. These approaches work on gaining information which is freely available to the public, and on gaining information freely divulged by the individual about their identity. While this type of information is not confidential and does not lead to direct financial gain it can be used to improve or enable identity fraud in conjunction with illegally obtained information. For example, if a person's account number was obtained through going through their bins, this piece of appropriated information could be used in conjunction with their mother's maiden name or the name of their father's school to enable online bank fraud.

Legally obtained information can give illegally obtained information a context, but it can also be a more covert and harder to detect approach to identity theft and identity fraud. Legally obtained information can be separated into two types: freely available information, and freely divulged information.

Freely available information

The first example of freely available information is a person's birth certificate. This document is a record that notes a person's name, names of that person's parents, and the date of their birth. In terms of the information provided, it is quite basic; it notes the beginning of an identity and places the identity in context with that of others. This is the first paper proof of someone's existence. Records of birth are kept in a register but copies of entries in the register can be obtained; these certificates are given to the

parents of each child born and additional copies can be bought for £10, added to which, birth certificates other than one's own can be requested. Legitimate requests for copies of people's birth certificates do occur. People with an interest in genealogy, for instance, will use birth certificates to track their family tree. Birth certificates could be used to establish false identities, for instance when the birth certificate of a dead child is could be obtained and used as the basis for the creation of a new identity. This was illustrated in the book *'The Day of the Jackal'* (1973) by Fredrick Forsythe. Other certificates that are available are marriage and death certificates. By obtaining a couple's marriage certificate, a fraudster can discover the maiden name of the bride. Security measures used by financial organisations often rely on questions such as 'What is your mothers maiden name?' to verify identification.

Death certificates mark the end of the legitimate identity holder's use of their identity, but potentially, with this information, a fraudster could resurrect the identity. The writing of a will and the, employing of a solicitor is intended as a means of shutting down an identity, ending its use by anyone. Further to the existence of these records in the registers of Births, Deaths and Marriages, these events are often reported in newspapers.

As well as the recording of births deaths and marriages, other events are also required to be registered, such as the creation of a company or business. Records of these are kept at Companies House and can be freely obtained. These records list the owner's name and their place of residence. The electoral register is another source that can be freely viewed at public libraries and list any person who is registered to vote in a particular area and their place of residence. Due to the use of the electoral register as a source of information on where someone lives there have been changes to this service. Now there are two registers: one which is freely available for the public to view and a second which marks a person's address.

Other sources of information exist which can provide a person's address, thus linking a name to a location. An example is the register of company directors at Company's

House which can be viewed by the general public; the register shows the address of any director or head of a company. This register can be viewed for £2 and shows the name and head of any publicly listed company.

Records of people's involvement with social groups, or organisations are also available and can provide information on a person's history and aspects of their biographical identity. Membership of a school can be found on the website Friends Reunited, and this information can help in establishing the name of the school someone attended, which is often used as a security measure in online and phone banking. The importance of this information is its use in the credit industry as confirmation of identity. According to the Association of Payment and Credit Services (APACS) the use of these set questions, mother's maiden name, primary school etc., is becoming a security risk as the use of this static security is a danger when the information can be gained from other places.

Membership of the armed forces can be found in military records held by Vetrans-uk and the National Archive which holds military records from pre 1924. By looking at the register and records of the General Medical Council, it is possible to find out who has a medical licence in the U.K. Impersonation of a medical professional - known as 'quackery' in America - can be a lucrative business. Below are several examples of this type of fraud where people have stolen the identities of doctors. The General Medical Council provides an online alphabetical list of registered medical practitioners. The register provides the doctor's reference number, name, any former name, gender, year and place of primary medical degree, date of registration and registration status. It also provides any publicly available information about the doctor's practice history since 2005.

What the register of companies and electoral register show that is useful is a person's address; this can be used in conjunction with illegal methods of gathering and appropriating such as mail redirection and bin raiding. As noted above, another source available on the internet is the Friends Reunited website, which not only provides information on where a person went to school but also, depending on how much

information is put on the website, an online biography, so that where the person lives, whether or not they are married and what their profession is can be determined. Other online resources include 192.com which provides an online search engine to find people and where they live.192.com searches electoral registers, directory enquires, the register of birth, deaths and marriages and census records. As well as these examples of how to find information on someone it is also possible to look at directories such as Yellow Pages, Thompson online and any phone book.

Seeking out this type of information is not illegal or prohibited; if someone was trying to find someone else, a long lost family member or a friend they have lost contact with, these are the types of places they would look in. Indeed, the use of identity gathering techniques is often employed by people seeking missing relatives. According to the National Missing Persons Helpline (NMPH) and the Home Office there are about 210,000 people who go missing each year. According to the NMPH (2005) the vast majority of missing persons are found within 72 hours, but still thousands of people remain missing. The NMPH receives 150,000 calls per year and helps to resolve 70% of the cases they take. In cases of people who go missing the police tend not to get involved in the tracing of them unless there is an element of criminal activity or the missing person is classified as a vulnerable person (e.g. missing children).

As well as the work of the NMPH there is also the Salvation Army's Family Tracing Services who concentrate on reuniting blood relatives. Despite the efforts of the NMPH and the Salvation Army, the issue of missing persons is still an area which needs more attention:

> "Other specialised agencies, official and voluntary, deal with various aspects of the missing person's phenomenon but none has an overview of the problem as a whole. There is no central or single source of general or statistical information on a growing social problem which causes much distress to the absent and those they leave behind alike." (NMPH, 2005: 2)

The majority of information and research on missing people centres on cases involving children and teenagers. There is very little information on adults who go missing; however, according to research conducted by the NMPH in 2002 –

- Males in their late 20s are more likely to disappear than any other group of adults.
- Among those aged 60 years or over, the most common reason for going missing is dementia, or mental health problems.
- 28% of adults who go missing sleep rough, as do two fifths of young runaways.
- Adults are more likely to go missing if they are going through a crisis or a difficult transition, or if they are vulnerable due to chronic difficulties.

(NMPH 2005: 3)

Aside from providing help lines and support for people who have lost friends and family, the NMPH also uses age progression and reconstruction technology and databases to identify unidentified people, both alive and dead. As part of this service, the NMPH provides a website database of unidentified people.

Freely divulged information

While many forms of gathering and appropriating involve interception of information such as paper proofs of identity, a person's identity can also be gained through communication with the legitimate identity holder or someone associated with them. As part of everyday life, individuals will use their identity and thereby divulge information about themselves. The threat from this situation comes from people's belief that either the information is safe to divulge or the person being told this information is trustworthy. Divulging details such as name and age may seem innocuous but if someone has an understanding of how to use these details, this can lead to further information which could lead ultimately to identity fraud. This process is dependent on the skill and knowledge of the person seeking to steal an identity and the willingness of people to divulge information. The trend in using the internet as an online diary- known

as web blogs is a source of information about people and their lives which ultimately can lead to an understanding of their identity.

An example of the use of freely divulged information for legal purposes is the use of the skill of cold and hot reading. According to Carroll (2005) the skills of cold and hot reading are reputed to have been used by fake psychics and mind readers. It is the skill of eliciting information about someone through conversation so as to imply that this information was derived from another source. Cold reading is the skill of doing this without prior information about a person, hot reading is when a performer finds beforehand out information about the person they will 'read', and uses this in conjunction with what is said in conversation.

While there is not a great deal of likelihood of these approaches being used, these skills do illustrate how it is possible to elicit information from people without them being aware of how that information was gained.

The threat of identity related crimes is in part due to confusion over what is 'identity sensitive information'. Identity sensitive information is any fundamental detail about a person's identity which can allow others to assume that identity. While some questions are clearly going to be seen as 'identity sensitive' for instance asking someone what their National Insurance number is, other questions, such as asking someone what their mother's maiden name is, may seem innocuous but are also identity sensitive questions the answers to which can help someone else to assume the first victim's identity. Thus, information can be elicited through a number of clandestine methods but most information is available simply through discussion. Information which is used to establish identity has to be freely divulged in order for it to be effective, what is the use of having an identity if you cannot or will not use it?

In 2005 it was discovered that Drivers and Vehicle Licensing Agency (DVLA) personnel were selling personal details about individuals at the rate of £2.50 for each item. The information sold included names and home addresses and was available to

banks, solicitors, private companies and private investigators. The DVLA's sale of information was discovered by the Mail on Sunday and spurred a ministerial investigation into the practice. In a report by Turnbull (2005) it was said that:

> "The DVLA even admitted it was happy to sell the data to convicted criminals – and its approved customer list revealed one parking enforcement firm run by two men currently in prison for extorting money from motorists" (Turnbull .D, Oliver .J, 2005: 11)

Aside from reporting the practice of selling information, Turnbull and Oliver noted that the DVLA in 2005 sold 100,000 names of drivers each month. The DVLA argue that there are legitimate reasons for selling the information and people who are entitled to buy it. However, the sale of this type of information is clearly a threat with regard to identity fraud as the information can be a key resource in the gathering and appropriating process.

The use of all of the approaches mentioned here is not legally prohibited and while it is possible that they may enable identity fraud, the investment of time and effort is required before the information enables the theft of an identity. Obtaining information about a person this way will not directly access any information which is private or confidential to the individual. But this information may begin the identity theft process, and if used in conjunction with illegal methods of gathering and appropriating, the likelihood of success in stealing an identity will increase. Furthermore, there is no crime in gathering this type of information; companies that use telemarketing techniques often use lists of people to contact from looking at these types of sources. The use of this type of information by genealogists is also legal.

Social engineering and pretexting

Social engineering is a term used to describe the manipulation of people that can take place during instances of fraud. Social Engineering is a key skill used by those seeking to steal an identity. According to Bearman (2004):

> "In a system, there is hardware, software and wetware, wetware being the human element of the system. With million pound security systems and state of the art security technology, the first two systems may be impenetrable, but with enough patience and knowledge, a social engineer can use weaknesses in the wetware to trick an unsuspecting target into revealing sensitive information. Social engineering is a use of psychological knowledge to trick a target into trusting the engineer, and ultimately revealing information." (Bearman .R, 2004: 3)

Bearman has compiled a series of papers on social engineering in the form of a guide on how to become a social engineer. What is covered in his work are a number of different techniques that can be used to discover information on people and how to gain access to information. Included in these different techniques are the use of bin raiding and the use of internet resources to obtain information. But essentially what Bearman discusses is the act of manipulating people and deceiving them. Another name for social engineering is pretext and this refers more closely to the process of manipulation that goes on. With every piece of information held by social institutions such as banks there is an accepted process for accessing that information; social engineering and pretext is the technique of accessing information under the guise of a legitimate request for information. With regard to identity theft and identity fraud, social engineering and pretexting can be involved both in the obtaining of another person's identity and in the use of a stolen or counterfeit identity. The key to social engineering and to identity fraud is the use and manipulation of information. Identity thieves use their knowledge of how key pieces of information, such as drivers' licences can be used to commit identity fraud. Equally, social engineering involves understanding how requests for information or the processing of information are undertaken by people.

Arguably, anyone involved in identity fraud requires an understanding of social engineering, and can be considered a social engineer. It is difficult to declare that social engineering or pretexting is a legal or illegal method of appropriating or gathering information; certainly in cases of identity fraud, these techniques are used for criminal

ends, but these are it is not an inherently criminal processes or techniques of gathering information.

Illegal methods of gathering and appropriating

Illegal approaches to gathering and appropriating have gained a high degree of attention because of the effectiveness of these methods for providing information. What is important to note is that they represent interception of information and means of identification intended for the legitimate identity holder. Also, private or personal information can be held by third parties, and information can be stolen from these sources also.

Intercepting correspondence

The first illegal method is the theft of information intended for the individual who legitimately owns the identity. Intercepting correspondence intended for the legitimate identity holder allows the person trying to steal the identity to access not only information but also objects sent through the post. Examples of objects that may be sent through the post are parcels, credit and debit cards, cheques or money. The advantage of intercepting mail is that the holder of the genuine identity is unaware of its existence. Also, there is to a degree a guarantee that the information is of value to the genuine identity holder and that the information is intended for the genuine identity holder. Theft of conventional mail can be committed by stealing letters from a person's mail box or a person's mail can be redirected to another address or a post office box, so it can be checked for private information intended for the legitimate identity holder.

Gaining information from the post can occur through simple mistakes made by the postal service. In one case in Bangor U.S.A. (2005), a man and woman were sent the drug test results of two men, by accident. The letter should have been sent to a post office box in a place called Portage Lake but it was mistakenly delivered to a post office box belonging to Wayne David Broome in Eagle Lake. While the zip codes for each post office box were different, the numbers of the boxes were identical. This simple

mistake allowed Broome and his girlfriend Nicole Dufresne to use the two men's social security numbers and obtain credit cards and merchandise equalling $4,000.

Another approach involving obtaining mail is to investigate houses that have recently been left by previous residents to check if their mail has been forwarded or not. Often, if the mail forwarding service offered by the post office is not used, when a person moves house there is a chance mail will be sent to their old address. Potentially this can mean that private and confidential information is left at the old address. Theft of mail can be just as effective a method of gathering information as raiding bins. In one case, from 2005, a former postman called Dido Mayue-Belezika ran a massive cheque fraud operation that involved several members of his family and cost his victims £20m. The gang, lead by Mayue-Belezika defrauded thousands of people by intercepting cheque books as they entered the sorting office Mayue-Belezika worked at. Once he had the cheque books he would hand them to his brother in law Ishiaba Kasonga who would sell the cheque books to money launderers. While the operation run by Mayue-Belezika defrauded nationally £20million and the number of victims measured in the thousands, it was because the gang were targeting one community in North London that attracted the police attention. It was estimated that 1,300 residents of Golders Green were defrauded of as much as £5 million. It was the apparent targeting of this community which lead the police to Mayue-Belezika and 36 others, of whom 22 were charged across the U.K. In 2005, Mayue-Belezika was jailed for six and a half years, his brother-in-law Kasonga for three and a half years, and the others received sentences ranging from six months to three years. Through this criminal operation, Mayue-Belezika was able to make a fortune:

> "While using a second hand car at work, at home in his council flat in Malden Crescent he had an expensive entertainment system, designer clothes, and a Mercedes 4x4 vehicle parked outside." (BBC News, 2005: 1)

It is estimated by Postwatch that of twenty two billion pieces of mail sent each year, fifteen million items go missing, are misdirected or stolen. As a source of information,

the mail can be invaluable and as the case of Mayue-Belezika shows if thief is organised he/she can steal a vast amount of money. In a report for the BBC, one postman describes how easy it would be to steal someone's mail:

> "Paul, from Ruislip, who worked as a postman for 34 years, told the BBC it was "easy" to steal mail while on a delivery round. "When you're sorting in the morning, there's pigeon holes in front of you and one of those pigeon holes is the one you do for a walk. "So if you pick up some mail and it feels like something that's interesting like a cheque book, you can just throw that into your pigeon hole. "And then when you start throwing in the walk-off you just sort that out later on, you just take it with you. "If you find money in the bundle you were delivering, you could just put it back in the pouch," he said. He said supervisors in sorting offices were no deterrent to those bent on thieving. "If you're determined to pinch something, you can do it," he said. "It's not hard at all." (Shukor .S, 2005: 1)

As well as the potential threat from post office personnel, there have also been incidents of criminals stealing mail from, houses, mail vans and postmen/post women.

Bin-raiding

The other approach is to steal from people's bins, in effect gaining the same information after it has been communicated to the legitimate identity holder. 'Bin-raiding' or 'dumpster diving' relies on people believing that once the information is discarded in the bin no one will attempt to look for it.

In a study by the credit referencing company, Experian (2002), of residential bins in Nottingham Experian found that people were discarding valuable information without any effort made to stop third parties from obtaining this information. The study found that of the hundred of bins in the Nottingham area:

- "Only 14% of household rubbish bins contained absolutely no information of interest to fraudsters.

- Almost three-quarters (72%) of bins contained the full name and full address of at least one household member.

- On average, one in every five bins contained a whole credit or debit card number that could be linked to an individual and 80% of these have an associated expiry date. In more affluent areas (i.e. stylish singles and high income families), up to two in five bins (42%) contained a whole credit or debit card number that could be linked to an individual and 80% of these had an associated expiry date.

- Bank account details were regularly found in the sample and, on average, one in every five bins contained a bank account number and sort code that could be related to the full name and address of a household member.

- Only rarely were attempts made to destroy information. Just 8% of households throwing away full card numbers had made attempts to destroy the documents, and only 1% of households had been successful. Attempts had been made by 22% of households to destroy bank statements but only 7% of households had been successful. No attempts had been made to destroy three of the four benefit books found in the rubbish.

- One bin contained a signed blank cheque and another contained an used cheque book. From another bin, information was found about an individual's full name, address, date of birth, bank account number, sort code, employment details and medical information. They had also thrown away a whole benefit book, utility bill and other official letters that might be used to corroborate identity. Significant information about this person was contained in a complete passport application." (Experian, 2005: 5)

Experian in this same study also discovered that bin-raiding had been recognised as a serious problem in 80% of local authorities. More recent work on bin-raiding has furthered the work of Experian and given more recognition to the dangers it poses. Work on bin-raiding by the company Rexel U.K. has revealed that two thirds of the population of the U.K. are still failing to completely destroy confidential documentation and that 80% of the public do not own a shredder. (Rexel Press release 2006)

In a study of high street bank bins conducted by Scamsdirect and the BBC programme Watchdog, it was discovered that vast amounts of private and confidential information was discarded by high street banks. According to Scamsdirect, HSBC, Bank of Scotland, Nat West and Halifax had all failed to dispose of vital and highly confidential information properly. In their report, Scamsdirect discovered a wide variety of documents such as loan and credit card applications, account numbers and customers' telephone numbers. While the Halifax was thankful to Scamsdirect for their research according to Scamsdirect Nat West and the Royal Bank of Scotland have threatened legal action.

Due to the awareness raised by the media over this type of gathering and appropriating, many people have begun to shred important documents before throwing them away. In some instances, the importance of shredding documents has even lead to police forces offering to shred documents. An example of this was when in 2003 Humberside police in Bridlington offered to shred the general public's thrown away documents to ensure their safety (BBC News, 2003). As well as the police, local councils have also urged the general public to shred as in the 2004 case of Middlesbrough Council who, during a spate of bin bag slashing in Gresham, suggested that residents shred their documents as it was likely that thieves were rummaging through the rubbish for information such as bank statements and credit card slips (BBC News 2004). Even with this precaution it is still possible to reconstruct shredded documents. In response to this, new shredders have been designed which cross-shred documents into small squares instead of a series of long strips.

The value of this approach is not only that people abandon important documents, but also it can be argued that by throwing these documents away, people forget about them, increasing the likelihood that their theft will go unnoticed. Here the saying 'out of sight, out of mind' is particularly apt as this is what identity thieves rely on when gathering information from people's bins.

Shoulder surfing

Aside from monitoring information on people by methods outside their direct control, it is also possible to monitor people as they are using private or personal information. An example of this is the practice of monitoring people as they use personal identification numbers (P.I.N's) and this practice is known as shoulder surfing. In a report by Summers and Toyne (2003) for BBC Online the threat posed by gangs who used shoulder surfing to gain access to credit information is discussed. In their report, Summers and Toyne discuss the several methods employed by organised gangs who use this method to access credit and debit card details including account numbers, personal identification numbers and in some instances the actual card itself. Summers and Toyne note that this type of identity fraud costs banks and account holders millions of pounds each year. According to their report:

> "Cost of ATM Fraud
> 1997 - £8.2m
> 1998 - £9.7m
> 1999 - £12.2m
> 2000 - £18.3m
> 2001 - £21.2m
> 2002 - £29.1m
> Jan-Oct 2003: more than £30m"
> (Summers .C, Toyne .S, 2003: 1)

There are several various methods of committing Automated Teller Machine (ATM) fraud through shoulder surfing. The goal is to obtain the credit or debit card and/or the

personal identification numbers associated with them; in order to do this some identity thieves monitor the locations where people are most likely to use this information, namely ATMs. One of the earliest approaches used involved stuffing a plastic sleeve into the card reader on an ATM; this meant that when a customer went to use the ATM they would insert their card into the plastic sleeve rather than the card reader. Once this is done the thieves plan on the customer trying in vain to insert their PIN, at which point they can 'shoulder surf' for the number. The next step is to wait for the victim to go inside the bank to complain at which point they can go back to the machine and pull out the plastic sleeve (including the credit or debit card). At this point, the thieves have the card and the PIN and can access the account. According to Summers and Toyne, this is known as a 'Lebanese loop'. This approach in turn gave way to more sophisticated methods.

The goal in shoulder surfing is to observe the PIN number being inputted and to copy the information on the card. Initially shoulder surfers would physically have to watch over a person's shoulder, but over time, cameras and binoculars have been used to shoulder surf at a distance. Shoulder surfers have also used small pinhole cameras (often concealed on the side of an ATM) and special card readers which are attached to the front the ATM card reader. This means that as the customer inserts the card into the ATM, the card is run through the thieves' card reader first. Another approach involves coating an ATM's keypad with ultraviolet ink and getting a copy of people's PIN. Criminals have even gone so far as to buy or steal ATM machines and set them up so that they can more easily obtain information.

With the advent of chip and PIN technology and the spread of ATMs into places other than banks, the value of operating a shoulder surfing operation has increased. Organised gangs have been caught operating vast systems of shoulder surfing on several ATMs. According to the Metropolitan Police, shoulder surfing operations run by a Romanian organised crime group are a major problem in the U.K.

Gathering and appropriating information on the internet

With the introduction of the World Wide Web has come a new group of offences covered by the term 'cyber crime', and several new forms of e-commerce where identification through technology is very important. The use of identities on the World Wide Web is discussed by Mike Butcher in the Observer (April 27th 2003). Butcher highlights the increased use of e-commerce and the risks that are associated with it:

> "The Interactive Media in Retail Group, a UK e-commerce industry body estimates that 14 million British shoppers spent some £1billion at e-commerce sites in November – the most ever in one month in the U.K and a 95 per cent increase on 2001." (Butcher .M, 2003: 36)

Butcher highlights the case of Stephanie Poutney who became the victim of a cyber criminal who was using her credit card details to make online transactions at websites she had visited. This type of cyber criminal is referred to by Butcher as a cracker rather than a hacker. This is due to the difference in intent between hackers and crackers:

> "Poutney had become the victim of a 'cracker'. Hackers, by contrast, are computer enthusiasts who like to mess around with software and expose problems on the internet for benign purposes. By contrast, some crackers work in serious, organised gangs. " (Butcher .M, 2003: 36)

Butcher explains how crackers not only go after individuals but also companies in an effort to cause harm and steal money:

> "In September IT security firm Synstar estimated that over 1,000 UK organisations had been cracked into – almost a five fold increase on the previous years 225." (Butcher .M, 2003: 36)

According to Butcher the most common form of cyber crime is the theft of data, in particular the theft of data regarding identity. Among these details, credit card numbers

are of particular interest. Butcher goes on to describe how some companies choose not to report instances of cyber crime due to the difficulty in detecting this type of offence:

> "That it's hard to detect and rarely reported makes cyber crime the ultimate 'silent crime'. It presents a Catch-22 for businesses: they can report the crime, risk adverse reaction from customers and disruption to business, or stay silent, leaving police with no evidence and no argument to procure more resources for enforcement." (Butcher .M, 2003: 36)

Butcher notes that companies have allowed crimes to be committed against them without reporting these offences to the police. The concern here for the companies is the appearance that they are not in control of the information they have. If it became common knowledge that IT companies and financial institutions were not able to protect this information, then they would lose customers and shareholders, which would lead to an even greater financial loss.

Butcher also describes how the then Home Secretary David Blunkett established a National High Tech Crime Unit to deal with the problem of cyber crime. This unit deals with a variety of crimes covered by the term cyber crime:

> "The unit divides cyber crime into two areas. 'New crimes, new tools' includes crimes committed against computers and networks that present new opportunities to criminals, such as cracking, virus creation and 'denial of service' attacks. 'Old crimes, new tools' are traditional crimes supported by the use of the IT, such as fraud, blackmail, extortion, paedophilia and child pornography, identity theft, intellectual property crime and stalking. The unit deals with some of the biggest cases in the UK and some of the largest businesses in the world." (Butcher .M, 2003: 36)

Butcher goes on to describe how this unit has been criticised for looking at large companies and government organisations rather than small to medium sized companies

which are ill prepared to fend off any kind of attack by a cyber criminal. Butcher also highlights the deficiencies in the law and legislation regarding computer enabled crime. Butcher highlights the fact that the principal law governing cyber crime is the Computer Misuse Act of 1990, which was brought in at a time when few had access to the internet, or any idea of its existence:

> "...according to Bill Goodwin, specialist journalist with IT industry title Computer Weekly: 'Under the existing legislation, I can steal a PC and be prosecuted, but if I steal a database I can't be prosecuted. Those are two big areas the Home Office is known to be actively looking at, but they haven't reached a conclusion yet.'"(Butcher .M, 2003: 36)

One approach to internet based gathering and appropriating of information is the use of computer cracking (criminal version of hacking) or spyware. According to Berinato (2007), the potential for using the internet for commerce was something internet based criminals were quick to capitalise upon. Through the use of computer viruses by internet based criminals, identity theft and identity fraud has become an easier crime to commit. Berinato notes that in 2003 the first of many viruses designed to steal personal information from online sources was discovered. The programme was called Berbew and was developed by an online criminal who calls himself Smash, the co-founder of the International Association for the Advancement of Criminal Activity (IAACA). Berbew operated undetected for approximately nine months and stole 113GB of people's personal details. Berbew was a type of computer program called 'malware'. Malware are computer programs which interfere with the functions of computers and send personal information to internet criminals over the internet. After Berbew was contained, new 'malware' programs appeared using similar code but designed to overcome defences set up to contain Berbew. Since Berbew, Berinato notes that just as defences to protect against viruses and computer hackers are developed, new viruses appear. In one case of computer hacking from 2003, a cracker was able to obtain details of five million credit card accounts from Visa and MasterCard. The cracker was able to

break through the security of a company that processed credit card transactions for businesses. (BBC News, 2003)

Another aspect of computer hacking to enable identity theft is the use of spyware. Spyware is a type of computer program that can be sent to a person's computer; once there, the program makes a copy of every keystroke entered into the computer and then communicates the keystrokes to whoever sent the spyware. The aim is to gain copies of passwords and financial information from people.

The internet is a communication tool that has opened up a number of different areas for criminal behaviour. With regard to identity theft and identity fraud, the risks faced on the internet are much the same as the general risks posed by identity theft and identity fraud. The goal when attempting to steal someone's identity is to gain enough information about a person's identity so that when entering the identification process (in whatever form it takes) the impersonator cannot be distinguished from the genuine identity holder. While the internet offers a more effective approach to identity fraud, many of the methods used to defraud people that will be discussed later (phishing and pharming) can be committed using other forms of communication such as telephones or the postal service. What makes the internet so attractive to fraudsters is the lack of fundamental security and state regulation. The internet is an environment which transcends nations, and internet based criminals from one country can target people from other countries with ease. There are therefore great difficulties in policing as security has to be built into every website and that security may not be uniform in nature. As companies develop a presence on the World Wide Web they have become targets for criminals engaged in cyber crime.

Identity on the internet can involve information that goes beyond the personal identity and refers to a presence people have in large databases used by companies and government institutions. With the advent of computer technology and data-basing it is possible for a person's identity to be reduced to a number. Security on the internet can involve the use of information specific to an individual. Questions such as what school a

person attended or what their mother's maiden name is are ways for organisations to ensure they are communicating with the legitimate holder of an identity. The flaw of this system is that in order for it to be used on a large scale the number and variety of questions asked must be uniform. This form of security is relatively static which makes it easier for customers to use. However, this weakens the security system by allowing identity thieves to target specific pieces of information in order to steal an identity.

For example, a persons name connects them to a birth certificate which shows their parents' names, which leads to a marriage certificate which shows a mother's maiden name. This process and others can be used to discover information used on online security. It requires effort and an understanding of where this information is to be found, but it is freely available, and does not require much interaction with the individual whose identity is being stolen. One of the fundamental flaws of security on the internet is that it cannot provide the physical face-to-face confirmation of a person's identity. The internet allows for complete anonymity for its users.

Use of phishing and pharming

The three types of identity fraud based on the internet are phishing, pharming and the use of spyware. These three forms of identity fraud, while found on the internet, are not dependent on this form of technology to work.

Phishing involves using an e mail message, which for all intents and purposes looks like an official message from an internet based company. Other names for phishing are 'brand spoofing or 'carding'. The email message sent by people committing this type of fraud describes some circumstance which calls for the receiver of the message to send their personal or financial details to a web based company they frequent. In reality, the email directs the customer to another website that does not belong to the company in question but to the fraudster. This way the customer sends passwords, financial details etc to the fraudster, allowing them to steal that person's identity. The name phishing comes from the way this method of identity fraud is used, large numbers of emails will sent out much as a fisherman casts a net.

An example of this involved the online auction company e-Bay. Customers of this company were sent an e-mail saying that the company had lost that person's financial details and that they needed the details to be sent again to a website listed in the e-mail. The 'phishers' in this case sent out numerous spam e-mails, confident that at least a percentage of the people they sent emails to would have an account with e-Bay. This approach has a hit and miss quality to it, as fraudsters try to catch a few people by sending e-mails to a great many. The following are two examples of phishing emails sent to customers of Suntrust and PayPal:

Suntrust phishing e-mail

> "Dear valued Suntrust member,
>
> Due to concerns, for the safety and integrity of the online banking community we have issued the following warning message.
>
> It has come to our attention that your account information needs to be confirmed due to inactive customers, fraud and spoof reports. If you could please take 5-10 minutes out of your online experience and renew your records you will not run into any future problems with the online service. However, failure to confirm your records may result in your account suspension." (Landesman .M, 2007a: 1)

PayPal phishing e-mail

> "Dear PayPal User,
>
> We recently noticed one or more attempts to log into your PayPal account from a foreign IP address. We have temporarily limited access to sensitive PayPal account features. Allowing your account access to remain limited for an

extended period of time may result in further limitations on the use of your account and possible account closure.

If you recently accessed your account while travelling, the unusual log in attempts may have been initiated by you. However, if you did not initiate the log ins, please visit PayPal as soon as possible to log in and perform the steps necessary to restore your account access." (Landesman .M, 2007b: 1)

Pharming

Pharming is the misuse of Domain Name System or Servers (DNS). Rather than sending emails directing people to false websites, pharming involves establishing false websites in the DNS server so that when people try to access a particular website they are redirected to a false website. This form of internet based identity fraud is in some respects the 'bigger brother' of phishing. While phishing targets individuals trying to entice them to a website, pharming invades the network and forces everyone who tries to visit a website to go to the false website setup by the fraudsters.

While the threat posed by pharming has been defined, actual instances of this type of crime are rare. In January 2005 Panix – a large New York Internet Service Provider – was hijacked so that internet users who attempted to use the Panix domain were rerouted to a site in Australia. (Greenarmor 2007) On this occasion there were no reports of financial losses. In April 2005, Hushmail, a secure e-mail provider, was also attacked and users were redirected (Leyden 2005). There have only been a few reported cases of pharming but the major concern is that this type of activity enables other types of internet based identity fraud. For instance by establishing a fake website for a bank, fraudsters could gain access to customer's private and confidential information.

Other approaches to identity fraud on the internet include the use of technology such as 'spyware'. This is software that allows a person to target another computer and record all of the keystrokes made. This way a person's activity on a computer can be observed, their passwords copied, and the web based companies they use noted. The use of spyware has become such a risk that there is now 'anti-spyware' programmes that can be bought to protect computers.

All of these forms of identity fraud that are based on the use of the internet paradoxically do not rely on the existence of the internet. The internet improves the chances of success, but in each case, what is done specifically is not unique to the technology. People are deceived into divulging information in the belief that the person they are giving this data to has a right to it or need for it. These forms of identity fraud could be committed by using conventional mail, or the telephone; these fraudulent requests for information could even be done face-to-face, so that the actual request for information used in cases of phishing and pharming is not unique to the internet. What the internet provides that is so attractive to criminals is a higher degree of anonymity, the process is much faster, more people can be reached globally and the lack of understanding by the general public with regard to how internet fraud is committed means that people are often unaware of the dangers.

The methods used by hackers on the internet to commit acts of phishing and pharming are in many respects modern versions of documentation forgery. What forgers aimed to do was copy original official documents to the point where third party users could not tell the difference. What hackers create on the internet are forgeries of official websites and their aim is to deceive third party users into believing that the website is the genuine article. While the medium has changed, the goals and end results are much the same. Even though the impersonating of a company through pharming is considered to be in many respects the newest form of identity fraud, this type of criminal behaviour has been used in the past.

Use of corrupt officials

As well as obtaining information by targeting the individual, as is described above, information can also be gained by targeting organisations that have access to confidential information about individuals. Corrupt officials can be found in both public and private sector organisations and their collaboration allows criminals to access vast amounts of information on individuals without there being any need for direct contact with the victim.

In 2002, one of the largest fraud cases in America highlighted the danger posed by corrupt employees. This case involved three individuals who used access to credit information to commit identity theft. The reason they were able to attack so many people was due to one of them, Phillip Cummings, using his job at a software company contracted to the credit company Experian. Cummings worked at a helpdesk to steal credit reports from numerous credit companies. Once Cummings had obtained the information, he would hand it over to his accomplices, Linus Baptiste and Hakeem Mohammed for $30 per report. As of 2002, this scam had accrued 30,000 victims and had made the trio approximately $2.7 million. According to the United States Department of Justice (2002), this was the biggest case of identity theft in U.S. history.

The theft of information from call centres is also a serious risk to individual identity which people can do very little to control or stop. According to Christopher Franklin from the information intelligence consultancy, Detica, there is a great deal of risk involved in using call centres, with regard to identity theft. In particular, Detica notes the danger of using outsourced call centres:

> "Some security experts argue that all call centres environments are at equal risk, but we feel that outsourced ones are particularly vulnerable as trust is placed outside the company and personal data could potentially be exposed to unacceptable risks." (Detica, 2005: 1)

Franklin also notes that some businesses have taken measures to stop theft by their employees. He notes the example of BT which has banned mobile phones and PDAs from their outsourced call centres to prevent its employees from copying information as it comes up on their computer screens. Franklin does note, however, that there are still many areas that are vulnerable to the actions of unscrupulous staff members. The risk posed by collusion with corrupt officials is the one area individuals are limited in their ability to protect their identity. As the purpose of an identity is to allow an individual to

interact with society, it is inevitable that some aspect of a person's identity will be beyond their control.

Disasters and fraud

Information on people's identities can also be gathered by exploiting circumstances where conventional identification process have broken down, such as after natural disasters or terrorist attacks. In a report for the Times, by Steve Bird and Christopher Browne (2005), the use of identities of victims of the 2004 Tsunami by identity fraudsters is discussed. This report describes how efforts made by family members to find their loved ones who were lost during the Tsunami have been used by fraudsters to gain access to these peoples identities:

> "Mark Jones, managing director of Conversant Data, a British fraud investigation company, said: 'Criminals pick up the name, age and home town of tsunami victims from television and other news sources, then make up a similar birth date to find out more from credit reference agencies, the victim's local electoral roll or dumpster diving {searching dustbins} to get bank account and credit card numbers among other details.' 'As many of the tsunami victims were reasonably well off the crooks know they are likely to have good credit records and thus make ideal fraud sources'" (Bird .S, Browne .C, 2005: 9)

Duration of the gathering and appropriating process

Estimating how long it takes to commit identity theft or fraud is dependent on the type and quantity of personal information criminals have access to. Gathering and appropriating can be done specifically to steal one person's identity; given time and knowledge of the identification process, any identity can be stolen. When trying to protect any identity, an individual will try to limit access to the information discussed above. They will use shredders before putting any documents in the bin, they will use security programs on their computers. The goal in protecting an identity is to make the gathering and appropriating process so difficult that identity thieves will give up before they can get enough information to impersonate someone. It is possible that fraudsters

will target an individual specifically, but there is evidence from various cases of identity theft and fraud which suggests that fraudsters will try to gather information on a large group of people. The use of phishing emails and bin raiding for instance suggests a very broad approach to finding a victim. In a sense, they will fish for information until they get a vulnerable identity.

It can be argued that this is due to the improvements in communication technology. In the 1980s, the introduction of the fax machine meant that fraudsters implementing the Nigerian 419 could send out faxes to large numbers of people. This trend was continued with the introduction of the internet. Now, rather than looking into one bin or stealing one person's mail the internet allows fraudsters to send e-mails to find information about people (phishing) or send out spyware programs which copy people's keystrokes on a computer. In many respects it is the use of technology which has brought identity theft and identity fraud closer together.

Amassing information about people

In many instances of modern identity theft, the goal is to impersonate victims only to the point at which they proceed to commit identity fraud. The exception is when identity fraudsters seek to adopt a new identity (see wholesale assumption chapter 8) and therefore must do more than impersonate the victim.

The methods of gathering and appropriating information on people presented here are intended as a guide to the types of information which can be stolen and how it is taken. There may be other methods of gathering information on people which have not been covered here. However the methods presented here highlight the most well known or established methods of gathering information on people.

Conclusion – the criminality of gathering information on people

In this first stage of the progression, the methods used are separated into legal and illegal approaches. This distinction is an important one as it highlights how information which may form part of a security procedure may not in itself be a secure piece of information.

Illegally gathering information on people's identities through theft or deception has the advantage of being more direct; it provides the exact piece of information needed to compromise a person's identity. Legally gathering information on people requires more 'leg work' to develop the information into something that can enable the abuse of an identity.

In the next chapter we will consider the next two stages in modern identity related crime, namely identity theft and the process of impersonation and identity fraud and the use of misrepresentation.

CHAPTER 8

Modern Identity Theft and Identity Fraud

Introduction

In chapter the 7 the process of gathering information on people is discussed, in this chapter we will look at how information gathered on people is used to impersonate them. Additionally this chapter will examine how the process of impersonation found in identity theft has increasingly been used to enable identity fraud and misrepresentations in various identification processes.

Unlike the early examples of identity theft and identity fraud discussed in chapter 6, modern identity theft and identity fraud are closely related phenomena. The increased value and use of identities in commercial transactions has meant that using identity theft to enable identity fraud has become an effective approach for criminals to adopt.

As stated in the previous two chapters, this study differentiates between identity theft and identity fraud in terms of who the criminal in question is deceiving and how. In modern identity related crimes, the criminal is victimising individuals by stealing their identity, and the criminal then moves on to use that identity with others in society and thereby victimises them through misrepresentation of who they are. It is this dual act of victimisation which often confuses people as to the difference between identity theft and identity fraud. The end result of using identity theft and identity fraud together is the depriving of the individual and social institutions in society such as banks.

Modern use of identity theft

The key to identity theft is impersonation. Identity theft begins when the person seeking to steal an identity has gathered enough information to impersonate the legitimate identity holder.

The time and effort required to impersonate someone varies according to the quality and quantity of information obtained while gathering and appropriating information on a

victim. In some cases the identity theft can take a long time to achieve – for instance if only legal methods are used to gather information. The use of illegal methods of gathering and appropriating can mean that the identity theft is achieved quite quickly and completed in a short space of time.

The identity theft begins when the person stealing an identity believes they have enough information to impersonate the legitimate identity holder. At this point, the legitimate identity holder and the person trying to steal the identity can present enough information to a third party to claim ownership of the identity. To achieve this situation can be quite easy in some cases and almost impossible in others. The determining factor is the nature of the identification process the person stealing the identity intends to enter. An easy impersonation would be using someone's identity with a person or institution the legitimate identity holder has never been involved with. A difficult impersonation would be if the person stealing the identity wanted to be identified by a family member of the legitimate identity holder. The level of information that would have to be gathered and appropriated would make this impersonation very difficult, as would the problem of overcoming any physical differences.

How difficult it is to impersonate someone is dependent on the identification process the identity thief intends to try and deceive. Many identification processes have minimal security surrounding them. However, where there are resources such as money or access to services allowed to specific people only, confirmation is required in the identification process. Financial service providers and government agencies often require confirmation of identity. So if an impersonation is to succeed it must be durable enough to withstand scrutiny if the goal of the impersonation is to obtain something only the legitimate identity holder is entitled to.

Observation of identities

Often the degree to which an identity is observed by its legitimate holder and by third parties can determine how open it is to abuse or stealing. Credit reference companies provide reports on a persons credit status- how many accounts, credit cards, debts, loans

etc. a person has - and through this service it is relatively easy to establish whether or not someone's identity is being used by an illegitimate user. Other services have also emerged using new technology to provide people with the opportunity to scrutinize and observe how their identity is being used. The supermarket chain Tesco has offered a service where they will monitor the purchases of a customer who has a Tesco credit card. If the credit card is used to buy something that the customer has no history of buying, or is unusual in some way, then Tesco will inform them of the activity. Other forms of observation are simpler, such as scrutinising bills and account summaries for any signs that someone else has used the identity. However well scrutinised a person's identity may be, there is always a chance that the identity could still be used without them being aware of the abuse.

There are several techniques that can disguise the use of another person's identity. The first approach is to target someone who will not be able to observe or detect the abuse of their identity, for example deceased fraud (see case of Charles Stopford page 115) or the use of a person's identity in other countries (see the case of Derek Bond page 113).

Another possible approach is to subtly change the name of the identity being stolen, for instance the inclusion of a non-existent middle name or initial, or a slight alteration in spelling. If, for example, my identity was stolen and instead of using my name correctly (Tim Holmes), the thief, introduced a nonexistent middle name (Tim A. Holmes) or changed the spelling (Tom Holmes), this would further confuse and obscure the theft of my identity, as the legitimate identity holder would have to determine whether my identity had been stolen or mixed up with the identity of another person named Tim Holmes.

If there is no obscuring of the theft of an identity then the effects of its theft will be noticed and measures will be taken to stop the abuse. Therefore if there is no attempt to hide the theft of an identity, then the identity thief must act quickly. Theft of credit and debit cards or the abuse of bank accounts has lead to heightened security when instances of theft are reported.

Is identity theft really about identity?

As discussed in chapter 2, there are many aspects to a person's identity and it is debateable as to how much the criminal activities of an identity thief will affect a person's identity. While in early cases of identity theft, such as the case of Arthur Orton and his impersonation of Sir Roger Charles Daughty Tichborne, there was a need to take on the life of their victims, it can be argued that in modern cases of identity theft there is less need to take on an elaborate impersonation.

Modern identity theft – is it all about documents?

While the term identity theft (and the term identity fraud) implies that a person's identity is actively involved in the process, it can be argued that what is really at the core of identity theft is society's response to a person's identity. In effect, it is not the name that is important but what entitlement and status the name provides.

It can be argued that the establishment of entitlement and status has in the U.K. often resulted in a great deal of significance being given to paper proofs of identity. Arguably, in many instances of identity fraud, it is the fact that impersonators have had access to documentary proofs of identity which has been of more importance than the simple verbal claim of being someone. During instances of credit or debit card fraud where the aim is to copy the card and obtain the personal identification number there is very little interaction with the personal aspects of the victim's identity. It can be argued that this crime is more theft of data than identity. Equally, in instances of identity theft by illegal immigrants, it is not the personal life and information which is desired, merely the status of being a legal citizen of a particular country. When looking at the activities of terrorists with regard to identity fraud again it can be argued that the goal is not to co-opt a person's 'sense of self' but to ensure access to a certain area or to avoid detection.

The issue of how much identity theft has to do with the issue of identity is dependent on the perceived extent and nature of a person's identity. The above examples of identity theft may not have involved the theft of an individual's personal identity or sense of self,

but these are still instances of identity theft as they abuse a person's link to society or their social identity.

Being a victim of identity theft

> "Virtually anyone may become the victim of identity theft. Contrary to popular misconception, personal information is not just from affluent. Persons of even modest means may become victims of Identity theft. In most cases all that is required is good credit, which is what Identity thieves use to steal thousands of dollars in the name of the victim." (International Association of Chiefs of Police, 2002: 2)

When a person's house is burgled the effect is clear to see and the victimisation is apparent. During instances of fraud, it can be very difficult to detect that a crime has occurred not only on the part of the victim but also any organisations they contact.

There are several reasons for this. One is that as fraud often involves the identification process used by large organisations the actual crime can be hidden from view. If a fraudster changes the billing address on a bank account they have invaded, the victim can go months without realising a crime has occurred. It is the length of time between the commission of the crime and when the victim becomes aware of it that confuses the issue of victimisation with regard to identity theft.

Another point which confuses the issue of victimisation with regard to identity theft and identity fraud is the issue of loss. Through conventional forms of theft, the loss of property or money can be quite clear and visible. In instances of identity fraud, what is stolen can be quite abstract or even virtual. Accessing a person's bank account and transferring money from it can be done over the internet with no contact with either the bank or victim necessary. According to Lesley Malone, Information Officer for Victim Support:

"The statistical data that Victim Support collects shows the number of fraud victims we support, but does not unfortunately break the information down any further so it is not possible to tell whether these were victims of identity fraud/theft or other types. Fraud accounts for less than 1% of referrals to Victim Support overall, although it is part of our core service, (i.e. all Victim Support branches must offer a service to fraud victims). This means basically that information, practical help and emotional support as described in Victim Support's service model must be offered, to the specified standard, and branches must refer a victim on to another agency where they are better placed to offer the help or support required, and the person supported requests this.

Just to touch on your point about victims approaching us - most victims are referred to us by the police when they report a crime, and the number of self-referrals we receive is very low (around 2%). We are also aware that although there is a formal agreement with the police that they should pass on details on all victims (except some agreed exceptions) that this does not always happen in practice, and it may be that victims of identity fraud who report it to the police are not always referred to us, for whatever reason.
Lesley Malone"
Information Officer, Victim Support National Office
(Malone .L, 2006 see appendix 16 for original email)

According to the National Consumer Council there are several difficulties faced by victims seeking help with identity theft:

"Victims or relatives find themselves very much on their own, often with little support, having to deal separately with each company concerned to prove the deception and bearing all the costs of putting things right. Victims of ID theft have reported spending months clearing their names, being hassled by debt collectors, blacklisted for new credit, and experiencing sleepless nights and health problems caused by stress." (National Consumer Council, N D: 2)

Can you take a person's sense of self?

The issue of how much identity fraud or identity theft has to do with an individual's identity is debateable due to the differing criteria individuals apply to determine what their identity is. As discussed in chapter 2 an individual's identity is in part the product of society's efforts to identify and categorise individuals and the individual's efforts to present their sense of self to society. It can be argued that identity theft is more concerned with documentation and acts of impersonation. The degree to which a person's sense of self is affected by identity theft can be very minimal. A sense of self is one way of describing an individual's personality or their individual efforts to identify themselves.

When discussing individual cases of identity theft, there is often a gap of time between the commission of the crime and the victim becoming aware their identity has been stolen. It can be argued that the reason for this is that most instances of identity theft do not directly affect the individual's sense of self. As the individual's efforts to express who they are within their direct control any effort to usurp this control may be easily detected. However while there may be no direct takeover of a person's sense of self in an instance of identity theft, it can be argued that there will be an eventual effect on the individual's sense of self when their efforts to identify themselves are hampered or denied due to the actions of their impersonator.

Identity theft can be seen as simply an issue of stealing data or documentation. But it can also be argued that it affects a person's sense of self, and it requires the abuse of societal expectations through the use of impersonation and deception.

Benign impersonation

Impersonating someone is not necessarily a criminal endeavour; pretending to be someone else or deceiving people as to one's true identity is not a crime unless this deception involves official documentation or identification processes which prohibit lying about details of one's identity.

An example of non criminal impersonation might be impersonating a famous person, such as Elvis Presley. The goal is to impersonate and imitate rather than take control of the identity and change it. It is the control and change aspects of the identity theft stage which indicate criminal intent. Changing identity is fully permissible in the United Kingdom, in some instances such as adoption and marriage the change in name is expected.

Identity changing services

While the issue of changing names or identities is represented as part of a criminal act, the desire to change or alter one's identity does not have to be a criminal matter:

> "Identity theft was once a serious problem. Thousands of people around the world had their identification stolen and were forced to pay large debts created by others. Up until now, law enforcement agencies and the general public have viewed this situation as chaotic. But here at A New Identity, Inc., we feel differently. If someone really wants your identity, good! Let them have it. We can get an even better one for you. Why bother with credit card debt, car loans, and home mortgages when you can leave them all behind? All you need to do is complete our free evaluation form, tell us a little bit about yourself now, and who you would like to become in the future. We'll analyze your information, determine the best identity for you, and send you a confirmation profile of the new you. Your identity will come complete with all necessary proof of existence, and cross-referenced by local and federal authorities. Once you accept your new identity, you may begin to enjoy the new you."
> (aNewIdentity.com, 2007: 1 of 1)

This statement is from aNewIdentity.com (May,2007), a company based in America which offers people a service to enable them to obtain a new identity, effectively discarding their old identity. aNewIdentity.com offers its clients the opportunity to take the identities of other people and obtain fake academic qualifications. The website

promotes the changing of a person's identity as a means of evading debt or criminal records and of obtaining access to another person's finances. (No mention is made of the legality of their actions). Ultimately, aNewIdentity.com claims that taking on a new identity will:

> "Make your dreams come true, Become the person you have always dreamed of, Eliminate bad dept, Improve your credit rating, Remove criminal convictions from your record, Improve your wealth, Remove all public info associated with you, Prevent telemarketers from finding you, Never pay a credit card bill again, Acquire property and never pay for it, Create a legal ID for each of your multiple personalities, Earn a degree from any prestigious institution in a matter of minutes for a fraction of the cost, Boost your self esteem, Make others envy you, Only you will know you used this service, We respect your privacy and won't tell who you really used to be." (aNewIdentity.com, 2007: 1)

Another American website - www.ariza-research.com - provides information on how to change identities. Since 1995, this website has offered a book on how to change one's identity. It reports that the commonly known methods of obtaining a fake ID are not only ineffective but dangerous. According to Ariza, going to websites that offer fake ID cards is a waste of time as these sites are often trying to deceive people and will either not send fake IDs to their customers or will send poorer copies of IDs than they are offering. On the subject of obtaining identities from gravestones Ariza are even more sceptical:

> "...inexperienced identity changers attempt to 'borrow' the identity of a dead infant through a terribly worn out system called 'paper tripping'. They wander through cemeteries in search of the gravestones of deceased children and then attempt to resurrect a dead child's identity on paper and assume it as their own. This tired old system has been so terribly overused by career criminals that it's now the most dangerous identity changing system available! Why?
> Just how many other new identity seekers have visited that same gravestone before you? Do you really want to take the chance that you'll be sharing your

new identity with a cop-killer or someone on the FBI's top ten most wanted list? {I didn't think so!}" (Ariza-research.com 2006: 1 - 2)

Ariza claims to offer not only a safe way of changing identities, but also a quick way, claiming that new documents can be obtained within a couple of days. The knowledge offered by Ariza research is one example of the type of literature that is available on changing identities. Books such as *'Acquiring New Id: How to Easily Use the Latest Technology to Drop Out, Start Over and Get on with Your Life'* by Ragnar Benson (1987) and *'How to Create a New Identity'* which was written anonymously in 1987, show how to change one's identity without resorting to criminal or deviant methods. The underlying theme in these texts is the idea that identity is something that is open to alteration by individuals who seek to change their lives. All that is required is for people to develop the skills to alter their identity, and then they will be free to be whoever they want to be. The general view of identities by aNewIdentity.com and Ariza is that the obtaining and changing of an identity is a simple process we can all engage in. However, it can be argued that for many people an identity is an integral element of their life which should not be tampered with.

Modern identity fraud - the use of misrepresentation

A distinction can be made between the activities of modern identity thieves and earlier instances of identity theft. Modern identity fraud is also different in many ways to earlier forms and approaches to committing identity fraud. The most notable difference is the increased use of identity theft to enable acts of identity fraud. This is not to say that fake or fictitious identities are not still used to enable identity fraud.

Fake identities – works of fiction

Another approach to identity related crime involves the creation of a new identity or an illegal modification of a person's identity. Rather than gathering and appropriating someone else's identifying details and attempting to impersonate them, a new fictitious identity is created. This identity has no records and is not recognised by any social institution. The effectiveness of this approach is questionable; without the input and

acceptance of society, this new identity has no existence beyond the declaration of its existence by the person using it.

Without the approval or sanction of society, this identity has no official documents, so that copies or forgeries of documents such as birth certificates would have to be made. These copies would have severe limitations compared to genuine documents as they would not have a place in the official records. While they would possibly pass a cursory inspection (dependent on the quality of the forgery), they would not pass confirmation by any official database, unless that database was corrupted in some way and an entry was included. According to Oscherwitz (2005) another name for this type of identity fraud used in America is synthetic identity fraud. Oscherwitz states that:

> "In contrast to 'true name' identity theft, where a thief impersonates a real – life victim, synthetic identity fraud involves creation of a fake identity through the combination of real and false identity elements – a virtual Frankenstein monster." (Oscherwitz .T, 2005: 1)

Oscherwitz argues that the large majority of identity fraud committed in America involves the use of synthetic identities, citing statistical research from ID Analytics that state that of 300 million account applications, 88% of successfully opened fraudulent accounts involved the use of a synthetic rather than 'true name' identity. The reason for the popularity of this type of identity fraud is according to Oscherwitz the lack of a 'true name' victim:

> "Why does this massive source of identity fraud get so little attention? A partial answer is that it is difficult to track. Since synthetic identities do not correspond to one particular consumer, the fraudulent activity will never appear on any consumer's credit report. " (Oscherwitz .T, 2005: 1)

The term 'synthetic identity fraud' in many respects refers to the older use of identity fraud where there was no need to use a personal identity. Looking at the activities of

people such as Archibald Stansfield Belaney who claimed to be Grey Owl, or Dr James Barry, it can be argued that fictitious identities have been used historically.

The use of camouflage passports

The use of fictitious identities can also involve fake or false documentation; one example of this is camouflage passports. Camouflage passports are documents which refer to countries which either do not exist or no longer exist to issue passports. These passports are available over the internet and are marketed as novelty items. In instances of identity fraud, camouflage passports can be used to cross borders or prove identity. Below are examples of camouflage passports reported by the Isle of Man Financial Supervision Commission (2008):

Camouflage name	Real name
British Guiana	Guyana
British Honduras	Belize
British West Indies	Does not exist
Burma	Myanmar
Ceylon (Republic of)	Sri Lanka
Dutch Guiana	Surinam
Eastern Samoa	American Samoa
Netherlands Antilles	Collection of islands e.g. Aruba, Curacão, etc., that do not issue passports. Citizens of the islands have full Dutch passports.
Netherlands East Indies	Indonesia
Newfoundland and Labrador	Canada

New Grenada	Does not exist, although Grenada does.
New Hebrides	Vanuatu
Rhodesia (Republic of)	Zimbabwe
South Vietnam	Vietnam
Spanish Guinea	Equatorial Guinea
Upper Volta	Burkina Faso
Zanzibar	Amalgamated with Tanganyika to become Tanzania. Exists but does not issue passports.

(Financial Supervision Commission, 2008: 1-2)

Camouflage passports play on the appearance of legitimacy. Providers of these passports claim their products are not meant to enable identity fraud, but it is possible that these fake passports may be used to enable identity fraud.

Identity fraud during states of emergency

Aside from the use of a specific fake identity there is also the use of a fake archetypal identity. Examples of this form of identity fraud can be seen during states of emergency such as Hurricane Katrina. According to the Federal Bureau of Investigation, after hurricane Katrina in 2005 there were several cases of internet based fraud surrounding the aid operation. One case involved a man who claimed on online forums to be a pilot trying to ship aid into the affected areas. He defrauded people by asking them for money to fuel his flights to New Orleans:

> "He laid it on thick, posting descriptions on the new web site describing his alleged non-stop missions to hurricane-stricken areas. He'd seen dogs wrapped in live electrical lines. He'd transported a critically ill 7-month-old girl to South

Florida for transplant surgery. He'd flown his plane alongside Air Force One and both planes had 'tipped wings' over Louisiana. The stories were so compelling that in just two days he'd collected some $40,000 from 49 people in the U.S., Canada, Mexico, Europe, and Hong Kong. One contributor alone donated $20,000" (F.B.I Press Office, 2005: 1)

Illegally modifying an identity

As well as the use of fictitious identities, there are also illegal modifications of someone's identity. This can be seen most clearly in cases of people who claim membership of regulated or prohibited identities, such as members of the medical profession, or members of state agencies, such as the police or the army (see chapter 6). While the use of a fictitious identity does not involve the theft of another person's identity, it does involve misrepresentation as to the individual's true identity. This misrepresentation can be done for a number of the same reasons and purposes as those sought through the theft of another persons identity. The illegality of this approach is in the forgery of official documents, and the abuse of services or social institutions.

An example of this type of deception in the identification process is the activities of Gene Morrison discussed in chapter 2. Morrison, while retaining his 'real' name had adopted the persona of a forensic expert and lied about his qualifications. Morrison used this deception for 26 years before being found out. Deception with regard to qualifications and experience is a practice which some argue has become more popular in recent years. In a survey of 1476 workers by employment law consultancy firm Peninsula, 66% admitted to lying about qualifications and experience. 8 out of 10 of those who admitted to lying said they would lie again to gain a promotion or enhance their career. While the use of fictitious identities or illegally modifying an identity may not be identity theft, it is an abuse of the identification process. It represents a misrepresentation of a person's true identity, and on this basis it is included in the discussion of modern identity fraud.

Identity theft leading to identity fraud

Once a criminal has stolen a person's identity, in modern instances of identity crime the next step is to progress to commit identity fraud by misrepresenting the victim's identity. The misrepresentation begins after a successful impersonation. From this point on, there is a third party who believes that the person who has stolen an identity *is* the legitimate identity holder. From this point onwards, the person stealing the identity is developing the stolen identity in ways not intended by the legitimate identity holder. In a sense, this is when a person whose identity has been stolen loses control of their identity.

Misrepresentation can involve developing the stolen identity, for instance obtaining a passport or driver's licence or buying a property. Misrepresentation can also involve taking resources from the legitimate identity holder such as taking money from a bank account or state benefits. While identity fraud can and does involve the continued victimisation of the person whose identity has been stolen, the deception at this point has shifted to varying degrees from the individual to the providers of resources in society. The diagram below shows how some forms of identity fraud are heavily dependent on identity theft to enable them, while other forms of identity fraud do not require identity theft but are made easier through its use.

Types of modern identity fraud

The types of identity fraud shown in this study are in part developed from the categories developed by the Fraud Advisory Panel (2003). The first form of identity fraud discussed is the use of identity fraud to avoid criminal liability or prosecution.

Criminal liability for the actions of others

In the U.K., the most famous instance of this form of identity fraud is the case of Derek Bond, but there have been several other cases in which people have been held responsible for the actions of the identity thieves who have targeted them.

As well as facing punishment for the crimes of their impersonators, victims of this type of identity theft must also face the stigma attached to the crimes of their impersonators. Being labelled a criminal can mean more than the prospect of some form of state sanctioned punishment, it can involve persecution by the community. In the 2002 case of Dr Paul Grout, his impersonator used Dr Grout's identity to obtain child pornography.

As well as being a Senior Consultant at Hull Royal Infirmary, Dr Grout was also one of the east coast flying doctors who were first responders to many accidents and emergencies. However when he was arrested in October 2002 he became a social outcast. Dr Grout was arrested and his home searched, his computer and files were taken and not returned until 2004. The arrest took place after Operation Ore - an international operation investigating paedophiles - had identified Dr Grout as a suspected paedophile. The F.B.I. had tracked and linked Dr Grout's computer and credit card to a child pornography website. In the two years before the trial, Dr Grout lost his job and many of his friends drifted away from him and his wife. As the trial began in April 2004, it was revealed that a link could be made between Dr Grout's computer and the accessed pictures; however no images were found on his computer. With the F.B.I's detailed list of when the images were accessed, Dr Grout's only defence was his electronic day planner. This showed that Dr Grout was not physically able to access the images at the times noted by the F.B.I. In one instance, Dr Grout was attending a police custody officer training course.

During the trial a computer expert testified that Dr Grout was probably a victim of a cracker. It was revealed in an investigation by the BBC's Inside Out (2004) programme that Dr Grout's only crime was being careless with his passwords and wallet, and that his system was vulnerable to computer hackers. Inside Out went to a computer expert called Gary O'Leary-Steele. Mr Steele is a computer hacker who helps companies with online security issues. Through a simulation of Dr Grout's computer system the programme was able to show how it took O'Leary-Steele moments to break Dr Grout's security:

> "'It's not much more than clicking buttons really,' explains Gary. 'There's no elite programming that need to be done. Any user who knows computers could break a password like this.'" (BBC News, 2004: 3)

Dr Grout was acquitted of the four charges he was arrested for - two charges of attempting to incite the distribution of indecent photographs of children and two charges of incitement to distribute indecent photographs of children. The argument that someone had hacked into Dr Grout's computer and stolen his credit card details saved the doctor from imprisonment. However, according to Detective Superintendent Colin Andrews of Humberside Police:

> "I am satisfied that this was a professional investigation, that it was right and proper that we investigated the allegations and a full and detailed file was given to the CPS, he said. These were not trumped up charges." (BBC News, 2004: 1)

The arrest of Dr Grout left him without a job and stigmatised by the idea that he was a paedophile long before his trial or proof of his guilt was established.

Other cases of people having their credit card details stolen and used to obtain child pornography have been reported by the BBC in connection with Operation Ore. According to the BBC of the 7,000 people who were detected using credit cards on a website which provided child pornography, 2,000 spent many months being investigated before charges were dropped. According to Professor Ross Anderson from Cambridge University:

> "The police just didn't look for and didn't understand the evidence of wholesale fraud....And as a result, hundreds of people, possibly in the low thousands of people have been put through a terrible mill with threats of prosecution for child pornography." (BBC News, 2007: 1)

These forms of identity theft force people to not only face the consequences of their impostor's actions but also the social stigma attached to the crime. While it is a key element of British law that a person is innocent until proven guilty, in cases of identity theft the 'accused' have the added pressure of proving they were not involved in the first place, despite evidence to the contrary.

In America there have been several incidents of this type of identity fraud, and in some instances even after the victims have informed the authorities of the misunderstanding, they have still been arrested and detained. The experiences of Michelle Brown are a good example of someone using another person's identity to avoid prosecution (see case of Michelle Brown page 109).

Another example of identity fraud used to conceal criminal activity is discussed in Bob Sullivan's book *'Your Evil Twin'* (2004). Sullivan highlights the case of Malcolm Byrd who suffered for five years after a man was arrested on drug charges and used Byrd's name when he was detained by the police. This incident took place in a town near where Byrd lived and he became aware of the misidentification when the arrest was reported in the local newspaper. He reported the mistake to the police and the newspaper printed a correction. Despite Byrd's efforts to correct the mistake with the police, four months later Mr Byrd was stopped for speeding and he was then arrested for drug dealing (the crime his impersonator had been arrested for). While Mr Byrd had gone to the police to inform them of the mistaken identity the police had not removed his name from the computer crime database. The mistake was realised when the police checked Mr Byrd against the photograph they had on file. The effects of this case of identity fraud escalated; Mr Byrd lost half a day's wages from being arrested and later Mr Byrd lost his part time job as a nursing assistant because his employers believed he had lied on his application for the job when he said he had no criminal record. Months later Mr Byrd lost his full time job and was denied unemployment benefits because of his 'criminal record'. By the time he had cleared up the mistake over his benefits, Mr Byrd was informed that his driver's licence had been suspended for non payment of fines. Mr

Byrd's impersonator had continued to use his identity and pin his crimes on Mr Byrd. In response, Mr Byrd obtained court documents from the county district attorney

While it can be argued that identity fraud in the form of wholesale and partial assumption are the most invasive in terms of controlling an identity, identity fraud as a means of implicating another in criminal activity can be the most destructive to an individual's well-being. To be held criminally liable opens the individual to being vilified and stigmatised for the actions of someone else.

Account takeover and false application fraud

The next two forms of identity fraud to be discussed are the use of account takeover and false application fraud. These forms of identity fraud are often highly dependent on personal identities.

Account takeover is a term which refers to instances where identity thieves steal an identity in order to gain access to an organisation with which the legitimate identity holder has a previously established relationship. Once this access has been achieved, the identity thief will abuse this relationship in some way. This approach can often involve the obtaining of information that an individual is required to keep secret such as Personal Identification Numbers (P.I.Ns). Often the account number or specific personal identity number on its own can be used without the need for a lengthy or thorough impersonation. During the sentencing of three men convicted of trying to steal £357,000 of tax credits from 40 people, the investigation discovered that they had obtained 37 national insurance numbers. In addition, they had used 11 fraudulent bank accounts, eight forged driving licences and nine credit cards, in an attempt to defraud the tax credit system. (BBC News, 2006) False application fraud is where an identity thief will use information gathered on their victim to start a new social relationship with an organisation such as a bank. An example of this might be the obtaining of a loan using someone else's identity (see below for examples).

Of all forms of identity fraud, false application and account takeover are the ones which have caused the biggest response from the credit industry. It can be argued that while identity fraud as a means of avoiding criminal liability is the most damaging, it is because of false application fraud and account takeover that identity fraud has become such a widespread phenomenon. The goal here is to gain access to people's bank accounts, credit and any type of money a person is entitled to through displaying their identity. Through the use of technologies such as the internet, it has become possible to victimise large numbers of people and shorten the process of impersonation.

How noticeable the abuse of the identity is in cases of false application fraud and account takeover, is dependent on the amount of money taken and how quickly this is done. The theft of a few pounds stolen periodically over time may go unnoticed. However, the taking of all of someone's money will immediately alert the individual to the theft of their identity. Taking someone's money through account takeover can be done by simply taking money from a cash machine, or by going into the bank; however both of these approaches leave the thief highly visible to any security the bank has. Money can also be taken by transferring the money from someone's account into another account. The use of phone and internet banking means that the thief can transfer money from someone's account without going to the bank.

In some cases of false application and account takeover, the criminals involved will play on a weakness in a particular identification process or system. An example of this is the targeting of the HM Revenue and Customs tax credit website which took place in 2005. The website was used by fraudsters to make online tax credit applications; they used the stolen identities of 1,500 employees of the Department for Works and Pensions. (Thomas 2005)

Liability for fraud

In instances of account takeover where money is taken by someone impersonating the legitimate identity holder, victims are reimbursed by the bank or credit company that the money was taken from. This can lead to the assumption that people are not really

victims as they are not at a financial loss. However, in many instances the burden of correcting the activities of an identity thief can often be the responsibility of the victim or their family (in instances where the victim is dead, very young or very old).

Example of account takeover and false application fraud

An example of false application fraud is the case of Robert Scott (Curwen, 2006) who had his identity stolen and used to obtain a number of loans and accrue a number of debts in his name. Mr Scott was left in the situation of having to locate debt collectors and solicitors who were seeking payment for debts he was accused of. This resulted in Mr Scott's credit records being so bad that no credit or loan company would take him on as a suitable credit risk. Mr Scott's existing credit cards were also set at a higher interest rate. Another example provide by the National Consumer Council is the experiences of Elsa:

> "Elsa, from Stratford-upon-Avon, was called by a debt collection agency, asking her to repay £4,387 owed on her credit card. Elsa has never had a credit card and the date of birth quoted was wrong. She continued to be harassed, by letter and phone. She went to the police but they just said it was a civil matter and would not give her a crime reference number.
>
> Eventually she was referred to CIFAS and advised to get her credit record and put protective registration on it {protective registration ensures that CIFAS member companies carry out extra checks whenever anyone applies for financial services in that person's name}. Her credit record revealed a long list of fraudulent activity. Three months later she is still dealing with the debt collector." (National Consumer Council, N D: 1)

Below is an account of one such instance of account takeover from the perspective of the victim. During this instance of account takeover, it was possible to speak with the victim directly and accompany her during a visit to their bank to report the incident. At the request of the victim, she will be referred to simply as Mrs B.

This incident of identity fraud took place in January 2007; it was discovered by Mrs B while she was reviewing her accounts online with her bank. While reviewing the accounts, Mrs B noticed firstly a sum of £112 and then a subsequent sum of £65 had been taken from her account in order to balance an account with Betfare an online gambling company that Mrs B had never heard of prior to the discovery of the payment. Both payments were made within days of each other.

With the knowledge that her bank account had been compromised, Mrs B approached her bank seeking to retrieve the stolen funds and prevent any further withdrawals from her account. Mrs B elected to visit the local branch of her bank in person and was directed to speak to a member of staff there. Upon hearing that her account was being accessed by someone, else the bank officials first checked the accuracy of Mrs B's claim. Then they reported the instance of fraud to the banks online fraud unit and gave Mrs B a form to outline how much money had been taken. According to Mrs B:

> "The whole thing felt more like an insurance claim rather than reporting a crime." (Mrs B, 2007)

Because Mrs B felt that her claim had not received the attention it deserved, she reported the crime to the police in the hope that the theft of her money would be recognised as a crime. However while the police did take a report of the incident, they were not optimistic that they could catch the thieves who had stolen the money. The targeting of Mrs B's account had taken a short amount of time to commit, and it was only due to Mrs B's review of her accounts that the crime was detected.

The attitude held by staff at the bank and to a certain degree by the police also suggests a sense of defeatism when it comes to instances of online account takeover; rather than treating the incident as a crime, the attitude seemed to be that it must instead be treated as an unavoidable hazard of using online commerce. Another point of interest raised by this incident is the timing of the account takeover. It is possible that one of the reasons Mrs B's account was attacked in January is that the theft of her money might go

unnoticed amongst other payments due to the increased spending over Christmas and New Year.

Identity fraud between family members

One area of victimisation which can be particularly damaging is when identity theft happens within a family. These incidents of identity theft often involve family members applying for credit or financial assistance using a relative's information. An example identity fraud within a family is the case of Elaine Hall and her impersonation of her younger sister Linda Cowan. According to Bruce (2007), Hall had stolen her sister (Linda Cowan) identity to conceal a criminal record for fraud.

Hall's impersonation of her sister involved using her sister's identity to secure work at a care home in Edinburgh under Cowan's maiden name – Linda Hall. The identity fraud also involved obtaining bank accounts, credit cards, store cards and a mobile phone contract in her sister's name. Eventually Hall was able to use her sister's identity to obtain a £140,000 mortgage for a four bedroom house in Livingston, West Lothian. Cowan was alerted to her sister's activities in 2003 when she was contacted about an overdue payment on a Ford Puma motorcar. After this initial discovery, it was revealed that Hall had been using Cowan's identity and credit to fund her purchases. It was estimated that Hall stole £250,000 from her sister. In August 2007, Hall was jailed for 15 months. After the sentencing Cowan was asked why she thought her sister had done it. She said:

> "Maybe she was jealous. She is older than me and maybe things should be the other way around, with me needing money from her. If that's true I feel sorry for her, this is what she ended up as. I do love her deep down but I can't stand the sight of her." (Cowan cited in Bruce .S, 2007: 1)

Theft of children's identities

As well as instances of identity fraud between siblings, identity fraud within families can also involve parents who use and abuse the identities of their children. Again, as

with identity fraud between siblings, the bond of personal trust between parent and child can make identity fraud easier to commit. Using a child's identity can be a very effective way for criminals to make money. While children may not have bank accounts or credit cards for identity fraudsters to exploit through account takeover, the fact that they have no bank accounts or credit history means that they have a perfect credit rating. This is something some people try to exploit.

In his book *'Your Evil Twin'*, Sullivan (2004: 47) reviews the case of Jeremy Potter and his use of identity fraud against his own children. According to Sullivan, Potter's activities were discovered by his ex-wife Rachel Soper. For a time after the divorce, Potter moved away from the town in Nevada that Soper lived in. After two years he returned with his new wife and step son. Sopers suspicions about Potter's activities were raised when she saw her ex-husband had bought a new car and furnishings for his house. Soper knew that her ex-husband and his new wife had a poor credit rating and could not afford any of the things they were buying. Soper's suspicions were further raised when Potter contacted her by phone and the caller ID showed the name of Potter's new stepson who at the time was nine years old. Soper later found out that Potter and his new wife had used the step son's identity on their electricity and home phone accounts. This lead Soper, who had three children with Potter, to suspect he may have used their children's identities as well. After performing a credit check on her seven year old son's identity, Soper discovered that Potter and his new wife had opened numerous credit card accounts and had made loan applications in the child's name. Potter had so completely abused his son's identity and credit rating that by the time Soper had performed a credit check, her son's credit rating had a reached a level equalled only by people who have declared themselves bankrupt. Potter had made no attempt to pay off any of the debts he had accrued in his son's name. When a credit card reached its limit, Potter simply applied for another one. Sullivan notes that Potter was able to do this because credit companies usually do not bother checking the age of applicants. Eventually Soper was able to convince the police to investigate and Potter was arrested and given a one year suspended sentence and two years on parole.

In many cases of identity theft and identity fraud there is no personal bond between the victim and the person committing the crime. In these cases, it can be argued that the bond of trust abused is a bond of social trust. But in cases of identity fraud between family members it is a bond of personal trust that the criminal abuses. This abuse in many ways is more damaging than instances of identity fraud where social trust is abused. But in terms of committing identity fraud, it can be argued that targeting family members is simpler than targeting strangers, and access to information is easier to achieve. Reasons for committing identity fraud against a family member can vary. In the first example discussed – the case of Elaine Hall – jealousy was raised as a possible cause, implying that perhaps the closer relationship and awareness of her sister's identity may have led her to commit her crime. But equally, the case of Potter and his abuse of his children's identities implies that identity fraud between family members may just be an issue of opportunity. Potter sought financial gain from using his son's identity; his awareness of his son's identity made the crime easier.

It can be argued that when committing identity fraud in the form of account takeover and false application, fraudster are not trying to adopt all of the identity or even pass themselves off as the victim for any length of time. This is what we would expect to see in more traditional forms of identity theft. But in modern cases of identity theft, it is the resources provided through an identity which the criminal is primarily focused on. Even so, the sense of being 'compromised' or 'vulnerable' to further attack does still exist, making false application and account takeover more than a clerical error.

Wholesale assumption and partial assumption

The next two forms of identity fraud are wholesale and partial assumption; these categories refer to people who are attempting to abandon their old identities and start a new life under another identity. The distinction between wholesale and partial is the number of identities involved. In cases of wholesale assumption only one identity is taken and used; in cases of partial assumption, criminals take on several identities in an effort to abandon their old identity. Wholesale and partial assumption can involve the use of dead people's identities.

The impersonation of Christopher Buckingham by Charles Stopford is an example of wholesale assumption as is the case of Christopher Clarkson and his assumption of Stephen Duffy's identity which was discovered in 2005.

The case of Charles Stopford is a prime example of wholesale assumption, as not only did Stopford maintain and develop the identity of Christopher Buckingham but he also abandoned the identity of Charles Stopford for 23 years. The reasons for committing identity fraud in the form of wholesale assumption, in this instance, were in many respects personal. This may account for the difficulty in detecting Stopford's activities, as his goal appears not to have been financial.

Another use for wholesale assumption is to avoid identification of a criminal past and an example of this would be the arrest of Christopher Clarkson in 2005. He was a member of a notorious gang of bank robbers known as the 'Stopwatch Gang', which during the 1970s stole about $8 million from 140 banks in Canada over a ten year period. Clarkson was one of two members of the gang who were facing charges on drug smuggling. During the hearings, Clarkson fled from Canada to America where it is believed he went to California and stole the identity of Stephen Duffy, a four year old boy who died in 1948. Using Duffy's identity, Clarkson went to Florida where he became a successful property dealer and lived for 30 years. Wigmore notes that when the Federal Bureau of Investigation finally caught up with Clarkson:

> "Special agent Ed Moreno said: 'He was definitely stunned. He didn't ask us any questions. He knew why we were there.' How much his wife Janice Caron knew about his past is unclear. Asked about his arrest she said: 'I just don't have anything to say right now.' Alan Brown, a colleague at the estate agency, said: 'The staff are all pretty shaken. Nobody had any idea he was anything but a normal guy'" (Wigmore .B, 2005: 1)

Wholesale assumption can be used by those seeking to distance themselves from a criminal record or some aspect of their past that impedes them in society. For example, someone may be a convicted sex offender who wants to work with children, or if a person who has declared bankruptcy may wants to conceal their past in order to obtain a bank loan. The goal is to distance themselves from the stigma or label attached to their genuine identity. This is in contrast to most other forms of identity fraud, where the goal is to obtain something from the other identity while still retaining a true identity. One approach to wholesale assumption is to use the identity of a dead person.

Deceased fraud – *Day of the Jackal fraud*

According to Credit Industry Fraud Avoidance System (CIFAS) and deceasedidentityfraud.co.uk, the use of dead people's identities in identity theft and identity fraud is a popular approach for identity thieves. Using the identities of dead people ensures that victims cannot complain about the abuse of their identity. Deceased fraud is sometimes known as *Day of the Jackal fraud*, referencing the use of identity fraud by the main protagonist in Fredrick Forsyth's book *'The Day of the Jackal'*.

Statistics on the use of dead people's identities compiled by CIFAS indicate that in 2005 there were an estimated 80,000 cases of identity fraud involving the identities of dead people.

According to BDO Stoy Hayward (2008), at any one time pensions are being paid to 70,000 dead people. In an article by Matthew Hickley (2002) for the Daily Mail, the theft of identities from babies is discussed. In this report, Hickley discusses how the identities of more than 1,000 babies who died before their first birthday have been used to create driver's licences, National Insurance numbers and passports for sale to illegal immigrants. Below are examples of victims' accounts of wholesale and partial assumption:

> "Mrs L explains, 'My mum died of cancer. We closed her affairs and arranged for mail re-direction. Within a few months we started to get letters from departments stores, credit card companies and debt collection agencies, saying

that mum had taken out credit cards, store cards and had failed to make repayments. I contacted each group and explained that my mum was dead, could not have taken out the debt and the people now living in my mum's old house must have stolen her identity. I was surprised at their reactions – from complete lack of interest to total suspicion about who I was.'

'I was very angry. Mum hadn't been well off, and had worked very hard to not get into debt, never taking out loans or credit cards and always paying her bills. I felt her reputation and her memory were being tarnished. I went to the police. To my absolute surprise, the police were not at all interested. They just told me I was not the person losing any money and to go home and forget about it! And so, for the last two years this has continued – only this week I've had another bill. My mum's name is still being used.'

Neither the police not any of the companies advised Mrs L of her rights as an executor and relative to ask for her mother's credit record. They didn't tell her about basic steps she could take to prevent ID theft and she had never heard of CIFAS until she told us about her case." (National Consumer Council N D: 5)

Another type of victimisation involving wholesale and partial assumption involves the identities of people whose ability to detect or protect their identity is impaired due to medical conditions:

> "Within the last month I have received correspondence from (a bank) telling my wife about her account. My wife has dementia and does not have the mental capacity to open an account. I have contacted (the bank's) customer service by phone on two different occasions and once by writing. Each time they said they would correct the problem. This last time, I was totally blown off and hung up on. I believe my wife may be a victim of identity theft for which (the bank) must take some responsibility. I need this matter corrected, and her name removed from any (bank) account." (This story posted online on 03/15/05)
> (Better Business Bureau, 2005: 2)

In instances of wholesale and partial assumption of a person's identity either the victim are kept unaware of the crime or are in a condition which makes them unable to report the abuse of their identity – such as in instances of wholesale assumption involving the dead or people with severe medical conditions such as dementia (as discussed above). This form of victimisation is arguably the worst abuse of a person's identity, as it removes individuals' right to control who they are. When this form of identity fraud is targeted at the dead, it is evident from accounts of family members that this abuse of a person's identity does affect others.

Partial assumption

Cases of partial assumption involve the assumption of several identities with the goal of abandoning the identity thief's genuine identity. Some partial assumers are those who have failed to maintain a wholesale assumption. The activities of F.W.Demara are an example of this kind of identity related crime. Demara took on several identities in an effort to abandon his own identity. Demara can be seen as a partial assumer because each of his impersonations and misrepresentations was found out, forcing him to take on a new identity.

A more recent example of partial assumption is the activities of Rasmus Kirkegaard Kristiansen who was a suspected murderer and identity thief from Denmark; he used the name Ronald Kirk and ten other false identities in order to hide in and amongst expatriates living in Portugal. (BBC News 1999)

Faking your death – case of John Darwin

Another example of identity fraud which can be described as partial assumption is the activities of John Darwin between 2002 and 2007. In 2002, John Darwin went canocing in the sea near Seaton Carew. Darwin was reported missing and a year later a death certificate was issued in his name. In reality, Darwin was not dead, but he had faked his death so that his wife could claim the life insurance. Darwin hid in his home after faking his death and in 2004 the couple decided to move abroad. At this time Darwin obtained the birth certificate of John Jones, a child who died in 1950. Using this identity Darwin

and his wife visited several countries and in 2006-2007 the couple began planning a permanent move to Panama. In September 2007, Cleveland police received new evidence that raised suspicions over Darwin's disappearance. In December 2007, John Darwin entered a police station in London claiming to have amnesia. His reasons for doing this are unclear; it may be that Darwin was aware of the police investigation and was trying to influence it. Darwin's story about having amnesia soon fell apart as pictures showing him and his wife in Panama several months earlier led to the prosecution of Darwin and his wife for fraud. Both were convicted and sentenced to six years in prison. The case of John Darwin is interesting as it represents someone who not only abandoned their old identity in favour of a new one; but also went back and tried to resurrect his old identity.

Partial Assumption as multiple false application fraud and account takeover

This form of partial assumption can develop from instances of account takeover and false application fraud, where the identity thief has in some way been able to construct a false identity around several instances of smaller scale identity frauds. It can be argued that the fraudulent activities of Frank Abagnale constitute this form of partial assumption as Abagnale routinely used different names. This form of partial assumption can be seen as multiple false application fraud and account takeover.

The key to the success of partial assumption, as with instances of wholesale assumption, is the absence of detection on the part of the victim. Unlike more short term instances of identity fraud, or incidents where criminals attack multiple identities at once, partial assumption requires a prolonged use of the identity. This increases the chances of detection by both the legitimate identity holder (excluding instances involving the deceased) and those in charge of policing the identification process.

Illegal immigrants and identity fraud

The goal in cases of wholesale assumption is the abandonment of one identity in favour of another. In many respects, this describes the motivation for illegal immigrants to use identity fraud. In chapter 3, the subject of illegal immigration and identity fraud is

discussed, outlining the activities of illegal immigrants and people smugglers. The use of identity fraud by illegal immigrants discussed in that chapter highlights how the goal is to obtain proofs of identity which can be used to allow someone to pass as a legitimate U.K. citizen. In a sense, illegal immigrants use identity fraud to abandon the identity of an illegal immigrant in favour of being identified as a legitimate U.K. citizen. In the cases of Charles Stopford and John Darwin the men had stolen the identities they used themselves; illegal immigrants can rely on people smugglers and organised crime groups to obtain a new identity for them.

Identity fraud as a means of breaching security

The final form of identity fraud which relies on the use of a personal identity theft is the use of identity fraud to obtain identification in order to overcome security measures. It involves obtaining forms of documentation which are relied on in society as secure or dependable proofs of identity. Examples of proofs of identity which are targeted during this type of identity fraud include driver's licences, passports and National Insurance numbers. There may not be an immediate financial gain to the adoption of that aspect of a person's identity, but this type of identity fraud is intended as a means of enabling other forms of identity fraud, such as false application fraud or using identity fraud to avoid criminal liability. This type of identity fraud is intended as a means of reinforcing any claim to another person's identity. The use of identity fraud to breach security is often associated with the activities of terrorists.

Terrorism and identity fraud

It was the attack on September 11th 2001 that highlighted the connection between terrorism and the use of false identities. This terrorist attack and the subsequent investigation highlighted how identity fraud has been used not only to enable terrorist attacks but also to fund terrorist activity. In 2002 testimony before the Senate Judiciary Committee Subcommittee on Technology, Terrorism and Government Information by Dennis M. Lormel, chief of the Terrorist, Financial Review Group at the Federal Bureau of Investigation, it was noted that:

> "...terrorists have long utilized identity theft as well as Social Security Number fraud to enable them to obtain such things as cover employment and access to secure locations. These and similar means can be utilized by terrorists to obtain Driver's Licenses, and bank and credit card accounts through which terrorism financing is facilitated. Terrorists and terrorist groups require funding to perpetrate their terrorist agendas. The methods used to finance terrorism range from the highly sophisticated to the most basic. There is virtually no financing method that has not at some level been exploited by these groups. Identity theft is a key catalyst fueling many of these methods." (Lormel .D.L, 2002: 1)

It is this connection between terrorism and identity fraud which has in the U.K. motivated an increase in the security surrounding various identification processes. Passport security and the introduction of identity cards are two examples of the concern that has been raised - not just by the threat of terrorism but also by the threat of terrorists who use false identities to enable their attacks:

> "Prior to September 11, governments and businesses were sensitive to identity impostors, but they viewed the problem as primarily a financial matter, that is, as a significant component of fraud. Called identity theft, statistics were gathered about its effect on businesses; hearings were conducted on its harm to individual victims and in 1998, federal legislation was passed to criminalize it.
> However, it was the events of September 11, and the investigation conducted afterwards, that awakened society to the fact that the criminal use of false identifiers and false identification documents is not just a significant component of fraud, but also of terrorism." (Willcox .N.A, Regan .T.M, 2002: 2)

In the September 11th attack, of the 19 hijackers, two utilised false identities during the attack – Abdul Azziz Alomari and Ahmed Saleh Alghamdi. With the help of Kenys Galicia, the two were able to obtain false identities and residency certificates which identified them as residents of Virginia. It was with these identities that they were able to board the planes they would eventually hijack with their co-conspirators. Aside from

the activities of these two terrorists, the others were also reported to have used false documents and identity cards. According to Willcox and Regan (2002), it is believed that all of the terrorists used false social security numbers. Social security numbers are comparable to U.K. National Insurance numbers and likewise are a key element of any identification process.

Willcox and Regan argue that while identity fraud has often been seen as the tool of con artists, the events of September 11th forced people to see it as a more fundamental element of most criminal activity:

> "The activities of the September 11th terrorist now cause us to realize that identity fraud is not just the tool of the con artist. It is, when properly recognised, indigenous to any criminal enterprise, whether it be drug trafficking, alien smuggling or cyber stalking." (Willcox .N.A, Regan .T.M, 2002: 4)

While identity fraud was used as a means of enabling the attacks on September 11th 2001, identity fraud was also one of the means by which al-Qaeda was able to finance the operation. According to Sullivan (2004):

> "A Spanish judge who presided over the indictment of eight suspected al-Qaeda members for involvement in September 11 says the group financed itself largely through credit card fraud. The terrorist cell, thought to be a financing hub for al-Qaeda, used stolen credit cards and false identities to move money and people around the globe. Perhaps $1 million was raised and moved out of the country by couriers to Saudi Arabia, U.S. investigators say." (Sullivan .B, 2004: 78)

However despite there being a connection between the use of identity fraud and terrorism, terrorists do not always need to use false identities: in the terrorist attacks in London on July 7th 2005, the terrorists did not use false identities and had no need to conceal who they were.

Theft of a business or organisations identity

The theft of a business or organisation's identity is distinctly different to the theft or defrauding of an individual's identity. When dealing with the theft or abuse of an individual's identity, the key point is that the identity should only be used by one individual. However, when dealing with the identity of an organisation – be it a business, charity or state organisation – the identity is designed to be used by multiple members of that organisation. Business identities can exist simultaneously in several countries, being used by different members of the same corporation.

Business identities

All companies in the U.K., have to be registered at Companies House; this and a number of changes involving the payment of taxes and the employment of other individuals, is how a business is formed. Beyond these parameters, a business can take any form in respect of the number of individuals involved, or the location of the business, and the goals and purpose of the business can vary greatly. This ambiguity over the nature of a corporate or business identity has been further exacerbated by the introduction of internet based companies.

There are two ways in which a business identity can be abused. The first involves stealing a business identity in much the same way an individual's identity is stolen. Impersonating a company can be carried out in order to gain individuals' account details or as a means of obtaining monies from someone by redirecting a payment intended to the legitimate representative of that company. This type of victimisation can be seen in instances of phishing and pharming as mentioned in chapter 7. While the initial goal in this type of deception is to gain access to the individual's account details, it is only possible by corrupting the organisation's identity.

In a report by Lague (2006), the experiences of Japanese electronics company, NEC, with corporate identity theft are discussed. According to Lague, after NEC employees at the Tokyo headquarters were alerted to the sale of counterfeit keyboards, CDs and DVDs bearing the NEC logo in Beijing and Hong Kong, an investigation into

counterfeiting was initiated. This investigation revealed that counterfeiters in China were making 'knock off' copies of NEC products and that they had also set up a fake NEC company:

> "Evidence seized in raids on 18 factories and warehouses in China and Taiwan over the past year showed that the counterfeiters had set up what amounted to a parallel NEC brand with links to a network of more than 50 electronics factories in China, Hong Kong and Taiwan." (Lague .D, 2006: 1)

The counterfeiters had set up their business as if it were a legitimate representative of NEC, the people who worked there were issued NEC business cards, shipping their products in crates that looked like authentic NEC packaging and the factories they used had NEC signs outside them.

Not only were the counterfeiters using the NEC company name and they were also producing their own products including entertainment systems, MP3 players, batteries and DVD players. League notes that in some retail outlets in Southeast Asia, the counterfeit products were being sold next to legitimate NEC products. According to Steve Vickers from International Risk:

> "... the NEC case demonstrated how piracy is evolving from opportunistic and often shoddy copying of branded goods to highly coordinated operations." (Lague .D, 2006: 1)

The NEC case represents the extreme of how criminals can use and abuse a company's identity.

Other confidence scams committed using business identities have combined the fraudulent use of individual's identities with the abuse of corporate identities. In 2004, an American company called T-Data discovered that its identity was being used by criminals to enable credit card fraud. According to Sullivan (2004), T-Data is a New York software based company, which does not accept and never has accepted credit card

charges. But in 2004 the owner of the company – Jeff Duhl – discovered that $15,000 worth of credit card charges had been accepted by his company:

> "A quick investigation revealed most of the charges had been made using stolen credit cards. Slowly, he caught on: someone had stolen a batch of credit card accounts, then stolen his company's name, set up an impostor version of T-Data, and rung up thousands of dollars worth of fake purchases. The 'profits' then deposited into checking accounts, it seems like the perfect scam." (Sullivan .B, 2004: 1)

As well as from T-Data, another 50 firms were targeted in this scam. By combining the theft and abuse of an individual and a corporate identity, the criminals had improved the process of gaining money from the act of identity fraud. In general when someone's identity is stolen and abused the biggest problem for the criminals is how to abuse the identity without being detected. By stealing the identity of a corporation the criminals in the T-Data fraud had tried to confound the company's ability to detect their abuse of people's identities.

Shell companies

The second approach is to set up a Shell company (also known as a paper company); these are fake companies that exist only on paper, not physically. Unlike the abuse of a legitimate company identity discussed above, this approach to corporate identity fraud involves creating an entirely fake company. This form of abuse involves the misrepresentation of criminals as legitimate business people, rather than the impersonation of another company.

In 2003 Devon and Cornwall police noted the appearance of a company called Data Protection Agency, claiming to be based in Crewe. This company was sending out letters to businesses based in the south west of England. They claimed that these businesses had failed to submit a notification to the information commissioner and if they did not send a £95 fee they would be liable for a £5,000 fine. The deception

employed by Data Protection Agency was in many respects a variation of an advance fee fraud, similar to the Nigerian 419 scam discussed in chapter 7.

Aside from the approach used in the above example, shell companies can also be used to manipulate investors and banks. In South Korea, in 2002, several businessmen were caught using shell companies to rig the stock market and defraud investors. 5,000 shell companies were initially created. The scheme involved creating fake companies that appeared to be well funded businesses; this would enable the gang to gain investment and bank loans. Once they had gathered enough money into the fake company, they would pull the money out of the company.

Just as in identity related crime targeted at individuals, the abuse of corporate identities can involve acts of impersonation leading to fraudulent activity; but it can also involve the development and use of fictitious corporate identities.

Limitations of the progression

The only thing this progression cannot illustrate is the amount of time it takes to commit identity theft or identity fraud. Previous definitions of identity theft and identity fraud have focused on the issue of time and have distinguished between identity theft and identity fraud on the grounds of how long someone's identity has been abused.

The issue of how long it takes to commit identity theft or identity fraud is a complex one which can confuse the process of defining the two types of crime. Issues which come into play when discussing the time it takes to commit identity theft or identity fraud include:

- the type of information used and how valuable it is to establishing proof of identity
- the skill of the criminals involved with regard to deception and manipulation of the identification process
- the use of technology both to steal information on a person's or corporation's identity and to facilitate the defrauding of social institutions

- awareness of the victims – both individuals in cases of identity theft, and social institutions in cases of identity fraud

Geography can be an important factor. The experience of Derek Bond is an example; Mr Bond's identity was used by Derek Sykes in the U.S.A. for over twenty years. Also the theft and abuse of NEC's corporate identity in China shows how identity theft and identity fraud on a global scale can be hard to stop or detect.

Conclusion

The purpose of presenting this progression is to explain how as time has passed, the use of identity theft to enable identity fraud has become a more popular approach. While early incidents of identity theft were targeted at notable identities, the expansion and development of identification processes has opened up more people to be targeted. It is these developments which have not only caused the redefining of certain activities as identity theft and identity fraud but which also explain why there appears to have been a statistical rise in the number of cases of identity theft and identity fraud. It can be argued that the combining of identity theft and identity fraud is a response to changes in society which the national identity card scheme is attempting to regulate.

CHAPTER 9

Identity Cards versus Identity Fraud

Introduction

To this point the emphasis of this study has been on defining identity theft and identity fraud. In this chapter the work on identity theft and fraud will be combined with discussion of the proposed identity card scheme, in order to determine what an identity card might do to prevent and/or detect identity theft or fraud.

The first part of this chapter is devoted to discussion of the current identity card scheme. It enlarges on points made in chapter 4 with regard to the introduction of a National Identity Card Scheme and what the scheme seeks to do. The aim of this part of the chapter is to determine what the identity card is trying to do. The second part of this chapter combines discussion of identity cards with discussion of identity theft and identity fraud. This part of the chapter will focus on the main question of this study: what effect might an identity card scheme have on identity theft and fraud?

Part 1

History of current ID card scheme

In order to discuss what the identity card scheme will do, it is important to discuss the origins of the current identity card scheme and the motivations for its introduction.

Where the idea for the ID card system came from is a point that does not have a straightforward answer. While it was initially presented by former Home Secretary David Blunkett, the concept of a National Identity Card has been suggested by previous governments, both Labour and Conservative. Both parties have suggested introducing identity cards and both parties have also opposed the introduction of an identity card scheme, citing the cost of introducing such a program and maintaining it.

As discussed in chapter, 4 ID cards have been used in the U.K. in the past, during the Second World War. At that time, they were accepted as a necessary measure for national

security. However when the war was over and the threat of invasion was gone, the system fell out of favour as it was seen as impinging on civil liberties. Since then, identity cards have been used as a means of security for companies and state agencies but never again have they been issued to all citizens.

While the ID card has not been reintroduced, there have been arguments for a return to the ID card system. The benefits of an ID card system are that they offer a simplified and universal form of identification. When applied to a national system such as the Welfare State or the National Health System it would mean a quicker and more streamlined administrative process. The original name for the current identity card scheme was the Entitlement Card Scheme, but this title was later changed. According to NO2ID (2008), this name was dropped in 2003 after criticism from the House of Lords; many lords refused to use the word 'entitlement'. But this first title is important in highlighting the purpose of the card: in an administrative sense entitlement is what the ID card seeks to establish – entitlement to the services each citizen has a right to. This is different to the use of the card as a security measure. According to Privacy International (2002), no European country has such a comprehensive or invasive identity card system. In this connection, Walton (2002) notes that European identity cards are not used to prevent crime; they are used as a means of establishing entitlement to government services.

Entitlement cards and identity fraud 2002

In 2002, a consultation paper published by the Home Office assessed how the then envisaged Entitlement Card would work and how the system might affect identity fraud. In this paper, much is made of the benefits to society that would come from having a general purpose card that could be used by the whole of society. This paper outlined the 'possible uses of the entitlement card' and it referred to the numerous ways this card could be used by various elements in society, both public and private. Ultimately, however, the concept of the entitlement card was that it would help the general public with the day to day process of identification:

> "Public services in the U.K. have developed their own individual ways to identify the people they need to serve and to determine what their service entitlements are. As a result, people need to provide the same information about themselves to many different organisations. They may also need to provide the same document such as a birth certificate a number of times. As well as being irritating, this can lead to delays in people getting services they are entitled to. At the extreme, people might not apply for services they are entitled to, especially if they have difficulty filling in forms or using the telephone." (Entitlement Cards and Identity Fraud, 2002: 27)

Initially it was thought that the entitlement card could be used in a similar fashion to a driver's licence or a passport. The paper also highlights possible layout for the card and the areas where it might be used. On the subject of identity fraud, the paper describes identity fraud as thus:

> "Identity fraud arises when someone takes over a totally fictitious name or adopts the name of another person with or without their consent." (Entitlement Cards and Identity Fraud, 2002: 39)

The entitlement card scheme aimed to improve security and combat identity fraud by providing what it refers to as:

> "...a higher level of assurance of a person's identity than existing documents..." (Entitlement Card and Identity Fraud, 2002: 30)

While this goal is both laudable and a good idea for combating identity fraud, the consultation paper goes on to explain the difficulties the scheme would face once it was set up. It makes no mention of how the system would guarantee it is providing a higher level of assurance of a person's identity.

The foundations of how this system will be setup are very important; it is the basis for any claim of security. Only by insuring that an entitlement card or identity card is in fact secure from the same kind of dangers faced by other identification documents, can it form the basis for a secure identification process.

The Entitlement Card Scheme faced many opponents in government and since 2002 there have been several changes in the legislation, most notably the change of name to the Identity Card Bill. One area where the identity card system has received significant alteration, particularly with regard to preventing identity theft or identity fraud, relates to the scope of the use of identity cards. While the card was intended as a universal form of identification to be used in all areas that would require identification processes, this issue of entitlement soon became a concern for critics of the entitlement/identity card scheme (see below).

The name 'Entitlement Card' proved to be unpopular and was replaced with the current title of 'Identity Card'. This change in the name of the scheme mirrored a further change in the aims of the identity card. These changes are explained in the Home Affairs Committees fourth report on identity cards (2004) by the then Home Secretary - David Blunkett:

> "Post-11 September 2001 I was asked on a number of occasions, starting on the end of the week of 11 September, whether I believed that we should have ID cards as a consequence of the attack on the World Trade Centre, and I said on record several times, and I still believe it, that whilst there could be a contribution towards countering terrorism this was not the primary purpose, and although it would be part of any such scheme it should not be seen as the sole focus. I went on to say that it was probably sensible, if we were going to move towards such a programme, to describe it as being part of entitlement- entitlement to services and benefits- which we had built up by the contributions we made and the mutuality that has stood us in good stead and is part of the National Insurance concept of the post Second World War settlement. I then

took that to the appropriate Cabinet committee the following January, that is January 2002. When we launched the consultation proper in the July it soon became clear that people did not like the term 'entitlement' card. They thought it should be an ID card, that it should be explicit rather than implicit, that it should give a clearer picture that it encompassed tackling terrorism and organised crime, and they believed that it should be more honest and transparent of the Government to do so, so in a nutshell we agreed after listening to the results of the consultation that that is what we should describe it as." (Blunkett cited in Home Affairs Committee, 2004: 24)

The change in title and the addition of the goals have lead to a great deal of importance being placed on the security of the identity card scheme. This is concerned not only with ensuring that the card itself is secure, but also the assurance that it is a secure form of identification, and is something that society can rely on.

Changes to current National Identity Card Scheme, August 2008

As of August 2008, there have been several changes to the proposed National Identity Card Scheme and the gathering of biometric data on people. One of the most significant changes to the National Identity Card Scheme has been plans to drop the compulsory obtaining of an ID card when applying for a passport. According to former Home Secretary Jacqui Smith (2008), plans for the identity card scheme are to allow consumer demand to drive the take up of the identity card. Speaking to the BBC Smith stated that gaining public acceptance of the identity card was as important as ensuring the system was as widespread as possible.

Other changes to the ID card scheme include changes to the national identity register. Originally, plans were for the national identity register to be contained on a single centralised computer database. Plans now are for several databases to be used to house the register. Ms Smith also announced that the identity card scheme is expected to achieve full coverage of the U.K. by 2017. These changes to the identity card scheme

mean that for at least the next nine to ten years the identity card will not be the only way for someone to identify themselves.

Identity card proposals and the law

The first area in which the identity card will affect the crimes of identity theft and identity fraud is in the new rules and legislation included in the Identity Card Bill. Included in the Identity Card Bill 2006 are changes in the legality of false documentation. The bill makes possession of false identity documents an offence:

> "It is an offence for a person with the requisite intention to have in his possession or under control-
> {a} an identity document that is false and that he knows or believes to be false;
> {b} an identity document that was improperly obtained and that he knows or believes to have been improperly obtained; or
> {c} an identity document that relates to someone else." (Identity Card Bill, 2006: 23)

The bill also notes that apart from the use of false documentation being a crime, so will be the creation or possession of anything that is used to create false documentation. The bill also makes it an offence even to have identity documents that are false, or improperly obtained, identity documents that refer to someone else or any of the paraphernalia used to create false documentation.

The punishment for someone possessing false documents or the equipment to make them – according to the act – would be a prison sentence upon successful conviction of up to ten years. For being in possession of false documents or improperly obtained documents, punishments laid out in the act vary from two year prison sentences to six months and the issuing of fines. The act defines false documents according to meaning laid down in the 1981 Forgery and Counterfeiting Act (part 1). Improperly obtained documents are defined thus:

> "an identity document was improperly obtained if false information was provided, in or in connection with the application for its issue or an application for its modification, to the person who issued it or {as the case may be} to a person entitled to modify it;" (Identity Card Bill, 2006: 24)

The combination of these provisions and the new legislation outlined in the 2006 Fraud Act is discussed in chapter 3. These provisions mean that not only are false representations illegal, but also the creating or obtaining of forged or false documents are also illegal, meaning that any attempt to present, create or use a false identity is illegal.

The proposed identity card scheme (22/06/05) also attempts to include the two objectives of improving provision of service and increasing security in the identification process in one system on a national level. The proposed security for this system will be a nationwide biometric register of people's identity. The nature of this system is designed to provide an ironclad form of identification which will be impervious to duplication or manipulation. An important element of how effective this system will be, however, will be the manner in which the identity card is used and checked on a daily basis. If the card is checked frequently and uses the safeguards provided by the biometric security, this should in turn make identity theft difficult to commit, and should improve the detection of false or fabricated identities.

However even in the 2002 Entitlement Card Consultation paper it is noted that relying on one form of identification is not the right way to combat identity fraud:

> "....-best practice in combating identity fraud stresses that organisations should not rely on a single source document or check to establish a person's identity. Organisations should make a number of checks from different sources. The range and sophistication of the checks will depend on the value of the product or service offered. Some commercial organisations have indicated their reluctance to undertake checks on identity – preferring to tolerate a level of fraud – unless

they can clearly identify a financial benefit which would outweigh the cost of the checks." (Entitlement Card and Identity Fraud, 2002: 30)

National Identity Register

The reason, it is believed that the identity card will provide a means of securing the identification process in the U.K. from identity fraud is that it intends to provide a secure database of information. Not only is the identity card supposed to provide key pieces of information on a person's identity it is also designed to provide information that it is in the public interest to know. But what does this mean?

A key part of the National Identity Card Scheme is the introduction of a National Register which will hold all of the relevant biometric security information and the personal details of individuals entered on the system.

The purpose of the National Identity Register according to the Identity Card Bill is to provide a means for individuals entered on to the system – people with ID cards – to prove facts about themselves included on the system. The National Identity Register is also responsible for providing a secure and reliable way for information about people included on the system to be accessed and confirmed. The parameters for accessing this information according, to the Bill, are if it is necessary for public interest reasons for this information to be accessed. The National Identity Register is a storehouse of biometric information and what the Bill refers to as 'Register able Facts'.

What is a Register able Fact?

Under the Identity Card Bill register able facts are determined to be the following:

1. "his identity;
2. where he resides in the United Kingdom;
3. where he has previously resided in the United Kingdom and elsewhere;
4. the times at which he was resident at different places in the United Kingdom or elsewhere;
5. his current residential status;

6. residential statuses previously held by him;
7. information about numbers allocated to him for identification purposes and about the documents to which they relate;
8. information about occasions on which information recorded about him in the Register has been provided to any person; and
9. information recorded in the Register at his request."

(Identity Card Bill, 2006: 2)

This list of register able facts focuses on not only people's identity but also their geographical location and history. The focus is essentially on who they are and where to find them. This is elaborated upon to include where they have been and occasions when they have interacted with other identification processes. The register also includes the possibility that people will want to include more information about themselves.

The Bill also elaborates on the meanings of the words identity and residential status to explain what is meant by these terms. Matching up the understanding of the Bill on identity and what is commonly thought to be identity fraud, will be important in explaining the possible impact of identity cards on identity fraud. According to the Bill, what is covered by the term identity are a person's name (including previous names), gender, age (including date of birth), and that person's physical characteristics.

This description of what an identity is according to the Bill is, arguably, simplistic. Rather than addressing sense of self or personal preferences for things like religion or political affiliation, the Bill's interpretation of identity adheres to the physical basics appearance and location.

What is in the public interest?

Much of the controversy surrounding the identity card involves how it will be used. According to the Bill, the parameter for why someone should be required to present their identity card, or have their information checked is whether it is in the 'public

interest'. The Identity Card Bill states that there are five meanings for the term 'in the Public Interest'. Something is in the public interest if it is:

1. "in the interests of national security;
2. for the purpose of the prevention or detection of crime;
3. for the purpose of the enforcement of immigration controls;
4. for the purposes of the enforcement of prohibitions on unauthorised working or employment; or
5. for the purpose of securing the efficient and effective provision of public services"

(Identity Card Bill, 2006: 1-2)

Looking at these various aspects of the term public interest, the final one listed above is a commonly used reason in other countries in Europe that have identity cards, but what distinguishes the U.K. identity card scheme are the other meanings applied to the term public interest. Both the use of the card for reasons of national security and for the prevention and detection of crime refer to the use of the identity card in preventing identity fraud and potentially terrorism (which is discussed later). In order to combat illegal immigration, the identity card will be used to control not only who enters the country (border control) but also by enforcing rules on employment it will potentially make it difficult for any illegal immigrants in the country already to continue living and working in the U.K.

Biometrics

Biometrics is the use of unique biological factors to test identity. The use of biometrics has increased in recent years, as technology has improved; however the use of biometrics is not new. While literature on the subject of biometrics covers various different aspects of physiology which can be tested and measured, the emphasis for this study with regard to biometrics is the issue of reliability and the use of three specific types of biometric tests in the National Identity Card Scheme, namely iris scans, fingerprinting and facial recognition.

Biometrics is the term indicating physical tests to confirm identity; an established form of biometrics is taking a copy of someone's fingerprints to confirm identity. More recent developments have included the testing of other physical features such as the shape of a person's face and the scanning of a person's iris. The effectiveness of biometrics in confirming identity has been an important issue in the development of security in the identification process. The basis for proclaiming that the current identity card scheme will be a secure form of identification is its use of a biometric security system. In reviewing some of the literature on biometrics, two key areas of concern have emerged, firstly the feasibility of using biometrics and secondly the elements of a person's biology which will be tested – namely fingerprints, iris scans and facial recognition technology.

Literature on the feasibility of biometrics

A feasibility study was conducted for the United Kingdom Passport Service (U.K.P.S), the Driving and Vehicle Licensing Agency (D.V.L.A) and the Home Office on the feasibility of using biometrics in an identity card scheme. According to this study biometrics is:

> "Biometric identification systems measure physiological and behavioural characteristics of a person, and use these measurements to reliably distinguish one person from another." (Mansfield .T, Rejman-Greene .M, 2003: 3)

According to Mansfield and Rejman-Greene biometrics can be used, to establish a person's identity and to confirm a person's right to access. Mansfield and Rejman-Greene note in their report that the proposed identity card system is the largest of its kind from a biometric point of view:

> "Such a system would be a groundbreaking deployment for this kind of biometric application. Not only would it be one of the largest deployments to date, but aspects of its performance would be far more demanding than those of

> similarly sized systems; such existing systems are either not applied in the civil sector or operate in countries where public acceptability issues are less prominent." (Mansfield .T, Rejman-Greene .M, 2003: 3)

In a report for the BBC, Twist (2004) looks at the proposed biometric system, and how it will be implemented. Twist interviews Mansfield in this report and discusses the usefulness of biometrics in the identification process. According to Mansfield, biometrics such as iris scans will be an accurate means of establishing identity, as long as there are provisions to deal with exceptional cases such as people with disabilities. Twist notes that:

> "In simple terms, explains Dr Mansfield, this means that one iris is more accurate than one finger in discriminating who is who. The added strength of iris recognition is that it never makes 'false matches', say experts. There has never been a documented case of an iris comparison mistaking one person for another. But the potential weakness of iris recognition is that it can fail to make a match at all." (Twist .J, 2004: 1)

A national trial involving 10,000 volunteers will be used to test how the new identification process will work. The first stage of this trial will involve reporting to one of the nationwide centres which is equipped with a booth designed to take recording of biometric data. These booths will record an image of a person's face, iris and fingerprint. Each of these characteristics is unique. Once they have been recorded, the second stage of this trial involves comparing the individual's biometric data with what has been recorded. According to Twist, this information will then be contained on a microchip which will be embedded in the identity card.

With regard to crime control, Twist points out that the role of identity cards in stopping terrorism will be marginal:

> "David Blunkett has admitted the scheme is not going to directly stop the possibility of terror strikes in the UK. But, he said, it would make a big difference to the work of counter terrorism and security services when it comes to verifying if people are who they say they are."(Twist .J, 2004: 2)

An article by Ali (2004) for BBC News Online reports the concerns posed by experts in biometrics and security systems. In this report, Ali quotes the concerns of a panel of experts at the Royal Institution in London. The concerns of these experts lay in the reasons for having an identity card scheme and the problems faced with implementing a system of this size:

> "Neil Fisher, director of security solutions at technology group QinetiQ, told the reporters the rationale of the Home Office for implementing the scheme - to deter illegal working and tackle immigration abuse, and strengthen the country's security – was in his view all wrong. Rather, it was a "golden opportunity" for Britain to set a new standard in our digital era, he said." (Ali .J, 2004: 1)

Ali also talks to Dr Frazin Deravi from the University of Kent who is sceptical about whether a large scale system would work, as a large scale biometric system has never been attempted before. The type of problems faced by this type of system include the breakdown of machines and any errors these scanners make; also there are some people who will not be able to use these machines. According to Ali, in some rare cases people with eye problems or damage to their fingertips will not be able to give accurate information to the biometric scanners. Dr Deravi further argues:

> "..the system could also be abused by way of false fingertips, photographs of irises or even masks," (Ali .J, 2004: 2)

Ali talked as well to Professor John McDermid of the computer department of the University of York, who believes there are positive reasons for having an identity card system:

> "'There are many instances where I would find an ID card useful,' said the professor.
> He argued that vital questions still needed to be addressed – such as whether the government could deliver within a reasonable timescale, what the detailed technological requirements were, and whether the system could really meet the government's objectives.
> At present, answers to these questions were decidedly hazy, he believed.
> 'The government doesn't seem to have worked out its requirements yet.
> There are many big and fundamental questions they don't appear to have an answer to.'" (Ali .J, 2004: 2)

Iris scans

Iris scans are the analysis of features in the coloured area of a person's eye which surrounds the pupil. According to the National Centre for State Courts (N.C.S.C.) there are more than 200 points on the iris that can be used for identification purposes. The N.C.S.C also note that idea of using scans of the human iris was first put forward by an ophthalmologist, Frank Burch, in 1936. However, it was not until 1994 and the development of algorithms by John Daugman and Iridian Technologies that iris scanning became a reality. It is argued by the N.C.S.C. that the usefulness of iris scanning lies in the uniqueness of the human iris:

> "The uniqueness of eyes, even between the left and right eye of the same person, makes iris scanning very powerful for identification purposes. The likelihood of a false positive is extremely low and its relative speed and ease of use make it a great potential biometric." (National Centre for State Courts, 2002: 2)

In a report by Mark Ward for BBC News Online (2003), the usefulness and effectiveness of iris scans is questioned. This report suggested that while iris scans would be able to confirm a person's stated identity effectively, this system would not be able to identify wanted criminals or terrorists due to the immense size of the database. The effectiveness of identification rates was also questioned in this report. Ward noted that:

> "In February 2002 the US Department issued a report that found wide discrepancies between manufacturers' claims of successful biometric identification rates and those seen in the field. The report found that iris recognition did better than most but one manufacturer's claims of a 0.5% false identification rate ballooned to 6% during the DOD tests." (Ward .M, 2003: 1)

Concerns also exist over the size of the proposed identity register database, Ward notes that according to the US General Accounting Office in November 2002 the largest iris scanning system had 30,000 records. According to Ward, it is unknown what difficulties may arise in implementing a system which has millions of people's iris scans stored on it.

For this report Ward talked to Professor Mike Fairhurst from the Electronics Department of the University of Kent who explained that the actual process of scanning people's information into the biometric database may prove to be difficult:

> "Tests of biometric systems by the UK's Communication Electronics Security Group have shown that people can take up to ten times as long to get through them than the existing passport checks." (Ward .M, 2003: 2)

Professor Fairhurst also points out that there are differing opinions globally over the acceptability of biometric scans. Ward gives the example of China, which has ruled out the use of iris scans over fears that they may cause damage to the eye.

Fingerprints

Fingerprinting is a method of identification and verification of identity which has been used by law enforcement organisations worldwide for more than a hundred years. Moore's *'The History of Fingerprints'* contains a discussion about the development of fingerprinting technology and its use. Moore explains that the use of fingerprints can be traced back to ancient Babylon and China where fingerprints were used in clay tablets and seals for business transactions. In more recent times, fingerprinting has been more widely associated with the investigation of crime. In the late 19th century, the development of fingerprinting allowed for the collection of copies of people's fingerprints. According to Moore, in 1888 Sir Francis Galton began studying fingerprint patterns as a means of identification. In 1891 Juan Vucetich, a police officer from Argentina, began using Galton's system to compile fingerprint files as part of his work. In 1892 Vucetich made his first identification using fingerprinting when he investigated the case of Francis Rojas. In the case, Vucetich identified that Rojas was responsible for the murder of her two sons and her own suicide, by using a bloody fingerprint Rojas left. During the 20th century, fingerprinting developed further with other countries including the U.K. relying on the accuracy of fingerprints. In 2002, the security provided by fingerprinting was brought into question. Japanese cryptographer Tsutomu Matsumoto demonstrated how using gelatine and digital photography equipment it is possible to deceive fingerprint scanners.

According to Leyden (2002), Matsumoto used gelatine and a plastic mould to create a false finger which fooled four out of five fingerprint scanners. Matsumoto then obtained other people's fingerprints using heated super glue to raise them on objects and then taking a picture using a digital camera. Using a PhotoShop programme to improve the image of the fingerprint Matsumoto then used a photo-sensitive printed-circuit board to etch the fingerprint into the copper of the circuit board. Matsumoto then applied the fingerprint from the circuit board to the gelatine fake finger. This provided Matsumoto with a false fingerprint which deceived fingerprint detectors 80% of the time. Bruce Schneier of Counterpane Internet Security said of Matsumoto's efforts that:

> "The results are enough to scrap the systems completely, and to send the various fingerprint biometric companies packing." (Schneier cited in Leyden .J, 2002:1)

The efforts of Matsumoto are important when discussing the use and role of biometrics. While biologically the factors being tested are unique and therefore reliable in confirming identity, the technology used to confirm identity is still open to being deceived.

Facial recognition

The development of facial recognition technology began in the mid 1960s. This technology involves the development of software which can measure and recognise a person's face. According to Johnson and Bonsor (2007), facial recognition software such as FaceIt which is developed by a company called Identix uses a person's unique facial features to identify them:

> "Every face has numerous, distinguishable landmarks, the different peaks and valleys that make up facial features. FaceIt defines these landmarks as nodal points. Each human face has approximately 80 nodal points. Some of these measured by the software are:
>
> - Distances between the eyes
> - Width of the nose
> - Depth of the eye sockets
> - The shape of the cheekbones
> - The length of the jaw line
>
> These nodal points are measured creating a numerical code, called a faceprint, representing the face in the database." (Johnson .R, Bonsor .K, 2006: 1)

Concerns over facial recognition systems in passports echoes the concerns raised over the usefulness of biometrics in identity cards. In a report for BBC News Online (2004), the light sensitivity of facial recognition scanners was discussed:

> "The BBC's Rory Maclean says unpublished studies carried out in Europe and the UK found the computerised scans failed in about one in 10 cases. The problems are apparently due to the technology's sensitivity to light conditions." (BBC News, 2004: 1)

Concerns were raised in this report by Professor Angela Sasse of University College London who is an expert in biometrics. Professor Sasse believed that facial recognition scans were not a practical security measure as there is a chance of the system misidentifying a genuine passport holder. According to Fiona Mactaggart a Home Office Minister is quoted as saying:

> "This technology is not foolproof. No country is looking just to depend on the biometrics technology. They are relying on all other things that are used." (BBC News 2004: 2)

With regard to biometrics, there is a great deal of confidence in the ability of iris scans to provide accurate information about who people are. This confidence is apparent in literature on the subject and the claims of experts on biometrics. However claims by critics of the scheme of difficulty in scanning certain people and the conditions under which these biometric scanners will and will not work raise concerns over the usefulness of this system. Another point of contention is the purpose of biometrically scanning people; the claims that it will help in the fight against terrorism or stop illegal immigration have been met with scepticism.

Data security in the U.K.

By introducing an identity card program in Britain, the government seeks to change the relationship between the individual and the state. Prior to the introduction of an identity card, the emphasis on initiating interactions between the individual and the state was on the individual. Registration for services or future access to services may be provided by the state, but it is dependent on the individual initiating the process. The identity card scheme will, initially, be voluntary and thereby replicate the old relationship between

the individual and the state. The intention was that in 2009 the system will be made compulsory with a fine of £2,000 for those who do not participate. This fundamental shift will eventually mean that the state will initiate the identification process. Whether or not this is a beneficial change, the implication of this change for civil liberty will be vast. As soon as the identity card becomes compulsory, the state will be in charge of saying who exists in Great Britain. This will mean that anyone who chooses not to participate in the identity card scheme will effectively be excluded from provisions of state welfare benefits and financial services.

The underlying issue here is control over identity. While individuals are in control they have the option to deceive others as to who they are. State control of identity in contrast is absolute, regardless of what individuals say or do, they cannot change their identity without sanction from the state.

Can you trust the government with your information?

Another question that must be asked when determining whether or not the identity card scheme 'should' be introduced is whether or not the government can be trusted with this information. The identity card scheme was introduced by the then Home Secretary David Blunkett and after he left the post of Home Secretary his successor - Charles Clarke - was also a proponent of the identity card, highlighting the possible introduction of a budget identity card. In October 2005, Charles Clarke introduced the 'budget' identity card which would cost £30. Unlike the identity card provided when renewing a passport or driver's licence, this card would be available at any time but without the added use as a passport or driver's licence.

However, Clarke was forced to leave the post after it was revealed that the Home Office had lost track of a number of foreign criminals who had been released from prison but not returned to their home nations. This incident highlighted the way in which administrative fumbles at the Home Office, over record keeping, could occur on a massive scale. After Charles Clarke came Home Secretary John Reid. His time as Home Secretary came under scrutiny with yet another mistake at the Home Office, another

failure to track 280 British nationals who had been imprisoned abroad. According to Tempest (2007), in this instance the police records were not updated by the Home Office so that the Criminal Records Bureau were unaware of the criminal records which included the details of 5 murderers, 25 rapists, 29 paedophiles, 17 other sex offenders, 29 robbers, 9 who were convicted of attempted murder and 3 who were convicted of attempted rape who had been imprisoned abroad. Again a large scale mistake was made, begging the question as to how secure the eventual National Register for the Identity Card will be.

The next Home Secretary was Jacqui Smith, and while there has been no reported change in the identity card scheme (August 2008) there has been a change to the structure of the Home Office which is being split, to an extent into two organisations. Aside from the Home Office there will also be a Justice Ministry which will be responsible for prisons, sentencing and probation.

Setting up a large scale database may seem like a good idea but unless security is guaranteed and mandatory, then it is a fundamentally flawed security measure. In 2005, it was discovered that 1,500 employees of the Department of Works and Pensions had had their information stolen (see chapter 8). The most recent discovery of problems at the Home Office with regard to tracking people (January 15 2007) came on the heels of plans to create a large Whitehall based database of people's personal information.

Function creep

The term function creep refers to the possible use of the identity card beyond the established reasons for its use. This term has been used in discussion of the identity card since the plans to introduce the Entitlement Card in 2002 were first discussed. In some respects, function creep has happened with every form of document identification in use today in the U.K. Drivers' licences are intended to prove who is allowed to drive a car, a passport indicates, your access to travel abroad, but both are used as generally accepted forms of identification. Paradoxically because there is no universal form of identification (such as an identity card), function creep is necessary with every other

form of documentation. So when people express concern over function creep with the identity card scheme, it is important to understand what exactly should be 'off limits' to the identity card and why.

Identity cards in the private sector

While the identity card is intended for interactions with state agencies and authorised private organisations; it is foreseeable that when it is issued not only will people use the identity card for interactions with authorised organisations but also with other unauthorised areas of society. It can also be argued that non-authorised organisations may begin to use the identity card as proof of identity, regardless of their ability to confirm the validity of the identity card they are shown.

In terms of using and accepting the identity card as proof of identification this would make the identity card similar to every other form of identification. This form of function creep is not really so different to what happens to every other document in use today. Where the issue of function creep becomes problematic is in terms of being 'required' to present the identity card. While this is expected when dealing with state agencies, it is possible that private organisations such as banks might require the ID card when someone is opening an account, or a company could make it requirement for job applicants to show their identity cards. The rules on the use of identity cards state that the individual must agree to have their identity card checked and verified against the National Identity Register. But it can be argued that if an individual denies an organisation the opportunity to verify the identity card, then the organisations may deny access on the grounds of security, or limit access on the grounds of the individual being a higher security risk. In the first Entitlement Card consultation paper it was suggested – as a positive advantage – that the card could be used in this fashion, in a sense becoming the only form of identification necessary or accepted in society. A popular phrase with regard to identity cards and the security they provide is: 'If you have nothing to hide you have nothing to worry about'.

The implications of this for civil liberties are of major concern to critics, not only in terms of the privacy issue but also with regard to limiting access to individuals have to society. In this respect, function creep is a major issue as it not only refers to the increased use of the identity card but also the increase in dependency on it by society.

Function creep will also have an effect on the usefulness of identity cards for crime prevention and detection. If the private sector relied heavily on the identity card in situations such as employment or in setting up of business relationships (accounts, loans, credit etc.) then it would be expected that the use of the identity card would ensure that things such as false applications could not happen (the card would be required to prove identity). The identity card in this scenario would become more than a secure form of identification; it would be a gatekeeper for all identification processes. This could happen if the function of the identity cards expands past its intended use. Equally, if the function of the identity card does not 'creep' into the private sector, the identity card will not become a gatekeeper for all identification processes. This will limit the usefulness of the identity card in the prevention of identity fraud. The identity card would only be effective at preventing crime against government agencies that require it as part of the process for accessing services. It is questionable how much crime this will prevent or detect. For example, while a percentage of fraud against the Department for Works and Pensions involves false identities, the majority involves people claiming benefits while working or claiming benefits they are not entitled to.

Part 2

Identity cards the potential threats and benefits

When discussing the interaction between an identity card scheme and the use of identity theft and/or fraud it is important to not only discuss not only how the identity card will affect identity theft and identity fraud. It is also important to discuss what threat is posed by identity theft and identity fraud to the identity card scheme.

This discussion will first address the question of what threat the identity card will face from identity theft and identity fraud, before considering the potential impact of the identity card as a preventer and detector of identity theft and identity fraud.

Identity cards and identity fraud – attacks on the ID card system

When discussing the role of an identity card in preventing identity theft and/or fraud, it is also necessary to consider the risk the identity card faces from identity fraudsters. In order for the identity card to be effective in preventing abuse of the identification process, it must itself be immune from corruption.

Risk in introducing the card – false application

The first point at which the identity card may face attack is in its introduction, and in possible false application fraud. One of the problems the ID card has which cannot be over come is that it is reliant to a certain degree on other forms of identification at its inception. According to the Identity and Passport Service, the identity card will rely on a 'biographical footprint':

> "Your 'biographical footprint' is simply the basic facts of your life, for example: name, date of birth and address. When you apply for an ID card, we will check your 'biographical footprint' against information held in other databases such as National Insurance or driving licence records. We will not rely entirely on written documents for this information {as they could be forged}. You will be asked to visit one of our local or mobile centres in person wherever possible. This will make it harder for someone to pretend to be another person when applying for an ID card." (Identity and Passport Service, 2008a: 1)

As seen with other forms of identification, there is a process of application in order to achieve the desired proof of identity, and this process can be corrupted. In the U.K., thousands of passports and drivers' licences are obtained through false application and applications using false identities as well as through theft. It was noted by the BBC in 2007 that the Home Office admitted that as many as 10,000 passports were fraudulently

applied for, and that more than a 1,000 passports go missing in the post each year. The identity card will not be the first form of identification a person receives and is reliant on other forms of identification. Therefore, for the identity card to be a 'secure' form of identification, the information it is based on has to be secure and immune to abuse by identity thieves. It can be argued that relying on a biographical footprint at the beginning of the process will undermine the secure nature of the identity card by assuming the secure nature of other proofs of identity such as passports or drivers licences.

Secondly, in order for an ID system to be accurate, it must be able to avoid ambiguity in the numbers of people it will cover and their ability to distort who they are. So for instance if you had a society of only thirty people and they were issued an ID card at birth, the likelihood that they could steal another identity, and be able to deceive the other 29 member of their society is slim. The U.K. ID card has the problem that it is not starting at year Zero; it is being patched on to a society that has a previously established identification system. The current identity card bill outlines a system where everyone over the age of sixteen would be eligible. This means that rather than being a system that starts from the beginning of an identity it is again being attached to a previously established identity.

With the incumbent identification system already open to theft and fraud, and the precise number of citizens in this society blurred by illegal immigration and migration in general, it is clear that the ID card system cannot guarantee accuracy.

For an identity card system to guarantee it is not being corrupted by some form of deception, it must be in place at the beginning of the identification process. While the idea of issuing identity cards at birth may seem impractical, it is the only way to ensure that the identification process is not relying on some other form of identification system.

The problem of introducing the identity card scheme is exacerbated by the prolonged introduction process of the ID card. Current plans are that the ID card will be compulsory and people will have to obtain one when they renew their drivers' licences

or passports. But with passports lasting ten years before renewal is necessary, and the ID card system planned for 2009 (the intention was that the card would be introduced for immigrants in 2008 first), it would mean that people who renewed their passports or drivers licences before 2009 could go ten years before needing to obtain an ID card. This wait for accuracy may be further held up by people who are opposed to the ID card making a point to renew passports and drivers' licences before 2009 and the introduction of the ID card.

While the National Identity Register will hold a record of everyone who has an ID card it cannot ensure that it is providing an accurate account of the number of people living in Britain today. In many respects, the ID card scheme is like a house built on foundations of sand. While it may appear solid and secure it cannot guarantee the information it is based on is accurate and true.

The consequences of this situation are that if someone who had committed identity fraud successfully wanted to, they could apply for an ID card and further validate their deception. This situation would allow the fraudster only to obtain an identity card in one name. It would limit the fraudster to committing one instance of identity fraud rather than multiple cases of identity fraud. However there are a number of instances where one instance of identity fraud is all that is needed, for example, in cases of wholesale assumption such as the case of Charles Stopford where the criminal in question has spent years trying to legitimise a 'biographical footprint'.

With regard to false application fraud it can be argued that the identity card is as open to this type of fraud as the passport and drivers' licence. In order to avoid false application there must be a process of ensuring that the person applying for the identity card is the genuine identity holder. The drawback of this is that any attempt to ensure that a person is the genuine identity holder will take time, and since this is a national scheme, it can be argued that this security measure will prolong the time it takes to complete an application for an identity card.

Breaking the security – account takeover

The second area where the security of identity cards will be tested is when criminals try to steal another person's identity card. This area of security will depend on the biometric security system installed on the card and the way this security measure will be used. This area of concern with regard to the security of identity cards is where the majority of effort has been placed. While false application fraud is an area that identity cards could have difficulty stopping, there are several reasons to believe that any attempt at a form of account takeover with regard to the identity card would face extreme difficulties. There are two elements of the identity card scheme which will make this form of identity fraud difficult to achieve, firstly the biometric security and secondly the National Identity Register. However these security measures are not always applicable as circumstances may arise where the identity card is used and relied on without the security measures being used. An example would be if the identity card was used in the private sector which has no way of confirming the biometric data or the identifying information on the national identity register. It is possible that forged or altered identity cards may be used.

Attempting account takeover with the National Identity Card Scheme would require some method of defeating or avoiding the biometric security. Equally, it would also require some means of avoiding detection of the takeover on the National Identity Register. In order to do this identity thieves may attempt to coerce people who work on the National Identity Card scheme or use corrupt employees to altering information or conceal the duplicate use of information. Another approach, which may prove to be the most damaging, is attacks by criminal computer hackers (crackers). The security of the identity card scheme is based on the accuracy of the biometric information held on the national register. As long as the information held on the register is accurate it can be trusted, but if computer crackers are able to access the register and manipulate the information held on the register, then the security provided by the identity card would be seriously undermined.

Equally it may be that identity thieves will attempt to avoid interacting with the security surrounding the identity card. This could be achieved by using forged or counterfeit copies of identity cards, in areas of society which do not have access to the National Identity Register. Companies without access to the National Identity Register cannot confirm if the identity cards presented to them are genuine or not.

The use of stolen identity cards

Another approach to the fraudulent misuse of identity cards is to obtain stolen identity cards and modify them for use by criminals. In theory, the theft of an identity card would not allow the person stealing the identity card to use the identity card successfully. In order to successfully use the identity card, the information on the stolen card and the national register would have to be altered. This would mean when the criminal had themselves and their identity card checked with biometric scanner, the machine would successfully match their biometrics with the details on the card's microchip and with the register. If the criminal only stole the identity card without altering the information on the register, they would not be able to match their biometrics with the details on the microchip and the records on the register. This would result in them not being successfully identified.

An example of how a biometrically secure form of identification can be stolen is the abuse of the e-passport system. In March 2006, a new biometrically secured passport was introduced by the Identity and Passport Service (I.P.S), in order to meet standards set by the International Civil Aviation Organisation (ICAO). The new e-passport is secured by the introduction of a microchip which holds the passport holder's photo and the personal details printed on page 31 of the passport. This information is used in conjunction with the Public Key Infrastructure to make the passport more secure in principle. According to I.P.S.:

> "The data will be locked down using a Public Key Infrastructure (PKI), which provides protection against encoded data being changed. PKI is a digital

encryption technology, which enables validation of the data as being genuine." (Identity and Passport Service, 2008b: 1)

By providing the Public Key Infrastructure a multinational database would be available – a Public Key Directory (P.K.D.). This would allow any of the 45 countries introducing the e-passport to check the chip and the biometrics on it. It has been argued that this security measure would make the theft or forgery of e-passports ineffective. Forged or stolen copies of passports would not show up on the P.K.D.

In 2008 during an investigation of the e-passport system, Boggan endeavoured to challenge the claims over the security of the e-passport. In his investigation, Boggan found that of the 45 countries who had signed up to the e-passport system, only five countries are using the P.K.D. Boggan also notes that Britain will not be using the P.K.D. until 2009. Until the P.K.D. is taken up by the other 35 countries involved with the e-passport system, confirmation of the information on the e-passport is done manually. This means that the protection against the use of stolen and counterfeit passports is compromised.

Boggan illustrated how compromised the security was by using computer expert Jeroen Van Beek, to clone the passport of 16 month old child, taking the information off the encrypted microchip and transplanting the information to another microchip. Van Beek then replaced the image of the child on the chip with that of Osama Bin Laden, and ran the microchip through a chip reader using the Golden Reader Tool software:

"At first, Golden Reader refuses to authenticate the new, altered chips. A digital key signature, a certificate of authenticity has been changed, and the reader is concerned. But Mr van Beek falls back on the work of Peter Gutmann from Auckland University, New Zealand, who found a way to programme another key signature into the chip. The IACO's reader software now accepts both chips as genuine." (Boggan .S, 2008: 7)

According to Boggan the lack of complete coverage of the P.K.D. means that cloned cards will appear authentic when used at passport control. Consequently, the theft and counterfeiting of passports still remains a threat to security. A similar situation could arise with the introduction of the national identity card scheme if the authentication process used is compromised in some way. If criminals are able to access the National Register, or if the register is not used effectively – as with the P.K.D.'s use with the e-passport – it can be argued that clones of the identity card may come into use.

Wholesale and partial assumption and the identity card

With regard to the identity card scheme it may be that those involved in wholesale or partial assumption may actively seek out an identity card. In instances of wholesale and partial assumption the goal is to abandon one identity in favour of another; in the case of wholesale assumption the identity card could prove to be a form of identification that identity thieves may actively seek out. In these instances of identity fraud the criminal is attempting to appear as legitimate as possible without open or easily identifiable instances of abuse. Identity cards may be attractive to wholesale assumers as the cards are intended as a secure form of identification which other identification processes will rely on. If a wholesale assumer was able to apply for and successfully gain an identity card it could be used by the assumer to dissuade anyone who has cause to question the legitimacy of the wholesale assumer's identity.

Equally, with partial assumers, it may be that gaining an identity card in another person's name may be an attractive option for people such as professional or organised criminals who wish to have a legitimate identity as well as the identity they use for criminal activity.

The biggest threat to wholesale and partial assumers with regard to obtaining an identity card is the reporting of their actions by the legitimate identity holders. The usual response to this danger is to consider using an identity which will not report the abuse, such as the identity of a dead person. However, as seen in the case of Charles Stopford and his impersonation of Christopher Buckingham, there are already methods of

detecting this type of abuse, by cross referencing with the registry of deaths. One possible phenomenon that may arise with the introduction of the identity card scheme is the application for identity cards by wholesale and partial assumers 'before' the legitimate identity holders have a chance to obtain an identity card.

As part of the identity card scheme, identity cards will be issued when people go to renew their passport or drivers' licence. As discussed earlier, current estimates are that it will be approximately ten years before identity cards have been issued to the majority of the U.K. population. It will be possible to apply for an identity card at any time before the renewing of a drivers' licence or passport is necessary and it is here that wholesale assumers may attempt to obtain a passport before the legitimate identity holder. If successful, both the individual and the system will face the dilemma of distinguishing the legitimate identity holder from the fake. There is also the possibility of mistaking the wholesale or partial assumption for a clerical error; two people with similar information whose files have been mixed up.

The problem posed by wholesale and partial assumers is different to the threat posed by identity thieves who are looking to defraud an identity. Wholesale assumers such as Charles Stopford can spend years amassing information and proof of identification to make their claim seem legitimate.

Social engineering and the identity cards

According to Finch (2005), one of the problems caused by relying on an individual form of identification is that people stop checking and confirming identity and rely solely on the technology of the identity card scheme. While the proposed scheme relies on advancements in security technology, according to Finch:

"What fraudsters know about is human nature. They know about people, they know how we operate, and they know how relationships of trust in which information is disclosed develop," (Finch cited in Amos .J 2005: 1)

Finch has been critical of the identity card scheme on the grounds that fraudsters will look to manipulate people who are involved in checking and confirming the identity card:

> "There is a worrying assumption that advances in technology will provide the solution to identity theft whereas it is possible that they may actually aggravate the problem," (Finch cited in Leyden .J, 2005: 1)

Finch's views on the identity card and the way criminals will react to it are based on interviews conducted with convicted fraudsters. According to Finch:

> "Studying the way that individuals disclose sensitive information would be far more valuable in preventing identity fraud than the evolution of technologically advanced but ultimately fallible measures to prevent misuse of personal information after it has been obtained," (Finch cited in Leyden .J, 2005: 1)

As seen with other forms of identification and more generally in previous instances of identity fraud discussed in chapter 5, the ability to manipulate individuals has often negated security measures put in place to prevent deception. People like F.W. Demara have found that there are circumstances where the conventional procedures for confirming identity can be avoided through social engineering. An example is Demara's exploits in the Canadian Navy and how he was able to enter it. While this is an old example, the increase in the reported instances of identity fraud since the year 2000, documented by CIFAS (see chapter 3), would suggest that this type of deception may still be possible. Accounts of social engineering reported in online forums (discussed in chapter 5) also imply that even with security measures in place people still find ways of 'conning' information out of people.

The security provided by the new technology included in the Identity Card Scheme may appear impressive. But ultimately the success of the identity card scheme will rely as much on the individuals charged with administering the security procedures as the

technology itself. While deceiving technology such as biometric security measures may prove to be impossible, it is clear that deceiving people is far from impossible.

What the ID card might do to modern identity theft and fraud

As discussed previously, in modern cases of identity related crime, identity theft and identity fraud are closely related activities. Using other people's personal information is a useful and easy way to commit identity fraud in the 21st century. In order for the identity card scheme to be effective in stopping or detecting identity related crime, it must be able to prevent impersonation and the duplicate use of personal information. If the identity card can prevent impersonation and identity theft then it will be harder for criminals to commit acts of identity fraud. By tying one person to one identity card, the scheme could prevent the use of multiple identities and detect anyone trying to use another person's identity.

The only hope the identity thief has is that they are able to alter the information on both the identity card and the National Identity Register, as discussed above, or that they will be able to avoid situations which would require the checking of the identity card.

Public sector identity fraud and private sector identity fraud

If the identity card scheme is successful in preventing people from using multiple identities as is the case in instances of identity theft, the next issue to consider is how many identification processes will rely on the accuracy of identity cards. The goal in introducing the identity card must be to prevent identity theft and thereby limit the ways people can commit identity fraud.

A distinction can be made when discussing identity fraud between fraud in the public sector (e.g. welfare state, immigration control etc.) and fraud in the private sector (banks, private companies). In both public and private sector fraud, identity theft is used to enable identity fraud.

Public sector fraud

Public sector fraud is an important area when discussing identity cards as it is likely that all government agencies will require the presentation of identity cards as part of their identification processes.

The first area of public sector fraud is the defrauding of state benefits, and benefit fraud is one of the areas that it is assumed identity cards will affect. Benefit fraud is where individuals fraudulently claim state benefits, such as unemployment benefit, housing benefit or state pension. The effect an identity card has on these and other forms of fraud in the welfare state is debatable. Those involved in the provision of state benefits will have access to not only the National Identity Register, but also any internal efforts to stem the growth of fraud such as the National Identity Fraud Unit of the Department for Works and Pensions (DWP). It is conceivable that there may be a positive effect on the levels of false application fraud and account takeover in the welfare system.

Critics of the identity card scheme have argued that the majority of state benefit fraud does not involve deception with regard to identity but rather deception with regard to eligibility. For example, fraud involving unemployment benefits often involves people who are working and claiming state benefits at the same time. This type of fraud would not be detected by the identity card, nor would the card impede people from attempting to commit this type of crime. In the London School of Economics study of the identity card project in 2005 the difficulty of establishing the exact numbers for identity fraud with regard to the benefit system are discussed.

The LSE Identity Project Interim Report (2005) study notes that figures on the levels of all types of fraud experienced by the Department for Works and Pensions vary from between £2billion and £5billion. According to the LSE, of these figures the number £3.5billion is taken as being an estimate of the level of fraud experienced by the DWP. Of this figure, fraud involving some aspect of identity fraud is thought to comprise 1% (£35million).

Health tourism

The term health tourism has been coined to refer to instances where people assume a false identity in order to enter the U.K. and obtain medical treatment on the National Health Service. As with other forms of fraud, obtaining accurate figures on this type of fraud is difficult. However, this type of crime is investigated by the National Health Service's Counter Fraud Service, which prosecutes instances of this type of fraud.

In 2005, the first case of health tourism was prosecuted; in this instance a 71 year old Egyptian called Albert Gilgris received heart surgery and prescription drugs on the N.H.S. Mr Gilgris had been given this treatment for free on the assumption he was a U.K. citizen when in fact he was not. Mr Gilgris was forced to pay £30,000 which covered the cost of his treatment. (Counter Fraud Service, 2005). In this type of identity fraud, it is the status of the individuals which is counterfeit, not necessarily the whole identity of the person; in some instances such as the case of Mr Gilgris it is the status as a U.K. citizen which is fraudulent. One area of concern has been the use of the N.H.S. by failed asylum seekers still living in the U.K.

Illegal immigration and illegal working

Another area of concern with regard to public sector identity fraud is one of the main reasons for the introduction of the identity card scheme, namely illegal immigration. When the first Entitlement Card Scheme was considered in 2002 one of the first reasons to be given for its introduction was the role it would play in combating illegal immigration:

> "By giving a clear indication that the holder of an entitlement card is lawfully resident in the U.K, a card scheme could be a powerful weapon in combating illegal immigration..... A universal entitlement card scheme would give greater credibility to legal migration routes into the country." (Entitlement Cards and Identity Fraud, 2002: 7)

This reasoning for the entitlement card carried on into later versions of the identity card scheme. The idea of using the identity card to combat illegal immigration in principle is a sound one:

> "The identity card scheme is intended primarily as a United Kingdom wide measure to help deter and control illegal immigration by helping to establish the nationality and immigration status of UK residents (...) " (Legislation on Identity Cards: A Consultation cited in Home Affairs Committee, 2004: 25)

By improving the government's ability to determine who is a legal citizen and who is not, it would be possible to limit what an illegal immigrant could and could not do in the U.K. Ideally the end result of this would be that if there is nothing for illegal immigrants to do in the U.K. they will either not come here or they would use legal means of migration. It was estimated by the Home Office in 2005 that there may be as many as 570,000 illegal immigrants living in the U.K. (cited in BBC 2005). However gaining accurate figures on the numbers of illegal immigrants is difficult as this is a highly covert community. Given that this is hidden community determining how the introduction of the identity card will work in practice can be difficult, as can determining what possible adverse effects there could be.

The attraction of being an illegal immigrant

One of the important elements of illegal immigration and illegal working is the 'pull factor' this is how attractive a country is to immigrants and illegal immigrants. The attractiveness of particular countries to illegal immigrants is dependent on the opportunities to make money in that country and the degree of safety, comfort and protection they can expect. In some instances, people will move through a series of countries to reach a particular country which is perceived as a particularly good place to go.

Another area of interest when discussing identity cards and illegal working practices is the role of employers. As well as the use of illegal workers by organised crime groups,

there is also the requirement for legitimate employers to ensure they hire legal workers. According to the Home Affairs committee report on Asylum Applications (2003-4) and illegal employment:

> "We believe that a significant factor in the problem of illegal working is the deliberate decision by some employers to break the law. We recommend that the Government should target such employers, who are not only easier to identify than those they employ but arguably more culpable." (House of Commons, 2004:83)

While it is unlikely that an identity card would succeed in stopping people from wanting to immigrate to a new country, the improved security to public services and access to employment would mean that living in this country as an 'illegal' immigrant would be more difficult. The impact of an identity card would be on catching illegal immigrants after they have arrived and attempted to establish a legitimate identity in this country.

Once in the country illegal immigrants would either have to overcome the ID card system and establish themselves as legitimate citizens or attempt to live in this country without interacting with government agencies or going anywhere that required the presentation of an identity card. Looking at experiences in other countries, there is reason to believe that while the basic idea of stopping illegal immigrants by introducing a national identity card may seem a good one, there is reason to believe it will fail. Countries with National Identity Card Schemes such as Spain still have problems with illegal immigrants. In Spain, it is estimated that there are between 500,000 and 800,000 illegal immigrants, mostly from Morocco and Northern Africa.

In America, the issue of illegal immigration has produced a new category of immigrant, 'the un-documented' immigrant, who while living in the country, in some instances paying taxes and in possession of all proofs of identity available to U.S. citizens, does not have U.S citizenship. This situation has lead to calls for an amnesty to allow 'undocumented' immigrants to receive citizenship and thereby official recognition.

In the U.K. the Home Office has operated a mass amnesty on three occasions, granting citizenship to 750,000 failed asylum seekers who had not left the country. In these instances the amnesty was enacted to clear a backlog of cases (BBC News, 2007). The effect of a general amnesty on any and all illegal immigrants in the U.K. is unknown; it can be argued that it would cause an influx of immigrants to the U.K. which would have a detrimental effect on state services such as the welfare state and the ability of the police and security services to operate. Equally it can be argued that providing an amnesty could help those immigrants who are beholden to organised crime groups or are too afraid of detection by the state to report criminal activity.

Role of organised crime, illegal immigration and the identity card

Who will try to beat the identity card scheme? This is a difficult question to answer, but it is reasonable to assume that organised crime groups and those involved in people trafficking will try to circumvent the identity card system or if possible attempt to beat it. Circumventing the identity card system is one reaction to the introduction of an identity card system. This could take place with the illegal immigrant community who are already trying to live in this country under a degree of scrutiny. The choice to try and circumvent the identity card would probably depend on the amount of false documentation that illegal immigrant had and how much they involved themselves with government services. If they were living in the U.K. with a set of falsely applied for papers (documents that by rights belong to someone else) or were using good quality counterfeit documents, they may be able to pass for a legal citizen. The identity card is not intended to be the only way to prove identity as the identity card will be introduced over time gradually as people obtain a new drivers' licence or passport. So the possibility exists that people will be able to operate as they have, pre-identity card.

It can be argued that by introducing the identity card the government will be introducing a quick and easy form of identification. Consequently, it is possible that anyone not using the identity card could come under greater scrutiny as the numbers of people with identity cards increase. They would in a sense become the exception to the normal

identification process when dealing with government agencies. This would take time and it is debateable whether or not detecting illegal immigrants is easier over time or if it gets harder. They may be able to gain access to better documentation or efforts to detect them may improve.

If the identity card does prove to be a success and is commonly used in society as a general proof of identity there would be an incentive for illegal immigrants to seek out counterfeit copies or to try and falsely apply for one themselves (see chapter 7 for false application). It would be difficult to try to live in a society which is heavily dependant on identity cards and identifying through identity cards would also be difficult. Either illegal immigrants would avoid contact with areas which rely on displaying the identity card or they would actively seek out some way of obtaining an identity card. The trade in counterfeit or falsely applied for identity cards could be a great source of income for organised crime groups. In effect the more of an obstacle the identity card becomes, the more organised crime will try to offer ways to either circumvent it or to obtain an identity card.

One possible result of the successful introduction of the identity card could be a reduction in the pull factor of the U.K. for illegal immigrants. Another possible result is that illegal immigrants will still come to the U.K., but due to the use of identity cards, illegal immigrants will be more reliant on those who have brought them into the country. Illegal immigrants could become more beholden to organised crime groups for a means to live in the U.K.

A final point is that made by critics of the identity card scheme who have noted that by introducing one centralised form of identification the government may be making identity fraud easier by giving criminals one specific form of identification to attack and counterfeit.

Security provided by ID cards against terrorism

Evidence to support the usefulness of identity cards in combating terrorism and the use of identity fraud by terrorists is limited. While much of the justification for identity cards has been based on its usefulness in stopping terrorism, identity cards have not been used in the U.K. or America as a method of preventing terrorism or detecting terrorists. It can be argued that even if an identity card scheme is introduced to the U.K., its usefulness in preventing or detecting terrorists is not guaranteed. The manner in which the identity card scheme will be used by the security services determines whether or not the identity card will in fact protect people from terrorism.

With regard to the recent terrorist attacks by al-Qaeda only the attack on Madrid in March of 2004 involved a nation where an identity card scheme was in place. The attack took place on the 13th March, when bombs were placed on trains in Madrid. In this attack a 192 people were killed and 2,050 were injured. After the attack the rail system around Madrid was shut down and security tightened. Eventually the four bombers were found in Leganes in South Madrid. Upon discovery, all four blew themselves up along with one police officer who was attempting to arrest them. While Spain has had an identity card scheme in place, the identity card did not play any part in detecting or preventing the attack. The example of the Spanish national identity card scheme does provide some insight into the potential drawbacks of the U.K. national identity card scheme. It can be argued that not only did the identity card fail to stop the attack in 2004, it has also failed to protect Spain from attacks by ETA, the Basque separatist group, who have been operating since 1959.

One of the main uses of identity fraud by terrorists as discussed earlier is as a means of breaching secure identification processes by using an alternative identity which the security services are unaware of. According to MI5 the benefit of introducing an identity card is that:

> "Many of the targets of Service investigations have multiple identities, and any system that makes it more difficult for our targets to use and maintain multiple identities would be welcomed." (Enquires Team, Security Service, 2007 see appendix 17 for original email)

In order for the identity card scheme to work in the U.K. as a method of detecting terrorists it must firstly be able to prevent the use of multiple identities, so that any terrorist in the U.K. could not enter a secured identification process without using their real identity. This approach is the main obstacle that an identity card scheme would provide to terrorists attempting to operate in the U.K. As seen in the attacks in America on September 11th 2001, every terrorist involved used stolen social security numbers and several used entirely false identities to succeed in their attacks. However looking at the later attack on London the terrorists involved were all using their own identities their success was based on the authorities not knowing they were terrorists.

In a speech given by Rachel North (2006) on of the survivors of the Kings Cross bombing and a spokesperson for the Kings Cross United group, which is a non political victim support group. North discusses the need for an independent public enquiry into the July 7th bombings, and criticises the argument given by the government that it would cost too much to have enquiry. As part of this speech, North discusses her views on the plans to introduce an ID card scheme to prevent terrorism:

> "It is a disgrace to talk about cost, when there is enough money to get the PM a private jet, to run John Prescott at £2million a year and to squander billions on ID cards, which will not stop fraud, nor identity theft, and certainly wouldn't have stopped the July 7 bombers, whom I understand were careful to look into CCTV cameras and to carry ID. Khan had 3 of the 4 carry his ID, so keen did he seem to be to achieve his posthumous fame as a martyr." (North .R, 2006: 4)

In some respects, the identity card scheme will work as a method of preventing and detecting terrorist activities provided that the security services have already identified as terrorists.

The second method of detecting terrorists with an identity card would be to consistently monitor the use of individual's identity cards, where they are and what they are doing with their identity card. Again this would require the security services to be aware that the individual is a terrorist to begin with. With regard to terrorism, the usefulness of the identity cards would not be as a tool to identify terrorists but rather as a means of excluding them from, and detecting them if they try to enter, locations and identification process where they could cause damage. For example, it would exclude them from airports or obtaining a passport, and if they do still attempt to enter they will be detected.

The ways terrorists could adapt to this situation is to avoid contact with the identity card scheme and any official identification processes that involve the use of identity cards. In effect, they would have to find alternative methods of gaining access or alter the manner in which they would attack. In response to attacks on New York in 2001, airport security and in particular passport security, has been increased to protect against the threat of terrorists attack. In 2006 an attempt to hijack planes in the U.K. failed. However, the attacks on London in 2005 and the more recent attacks and attempted attacks on Glasgow and London involved bombings on public transport and the use of car bombs implying that there is an alternative to hijacking planes as a means of attacking the U.K. With the recent attacks there has been increased speculation over the possible use of identity cards in the U.K. as a form of internal passport. This would allow the state to monitor the movement of citizens. The use of identity cards in this manner has raised several concerns with regard to civil liberties.

Private sector fraud

The effect identity cards will have on identity fraud against private organisations is dependent on the level of access the private sector will have to the National Identity Register. In 2005, plans were put in place to sell access to the National Identity Register to private companies at an initial cost of £750 with an additional cost of £750 for machines that could read biometric details. This initial plan was reported by the

Independent News paper and the BBC. In a report by the BBC then Immigration Minister Tony McNulty stated that:

> "...a verification process would take place, but denied private firms would be allowed to 'go fishing' for information. 'Verifying facts about an individual's identity is entirely the purpose of the database.'" (McNulty cited in BBC News 2005: 1)

According to the Identity and Passport Service, the current plans with regard to identity cards and the private sector is to allow access to the National Identity Register for 'accredited organisations' who will be able to verify information held on identity cards, but not to change or amend that information. This process is referred to as an Identity Verification Service, and the Identity and Passport service note that it will work at different levels according to the situation the card will be used in. They provide the following examples on their website:

- "for a basic transaction such as proving your age it could confirm simply that your card is valid
- if you are a foreign national applying for a job it could be used to confirm that the status of your visa allows you to work
- if you are applying to work in a position of trust {as a nanny for example} it could be used to confirm that you do not have a criminal record" (Identity and Passport Service, 2008c: 1)

The use of the identity card in the private sector is dependent on the acceptance of the individual. If a person does not want their identity card checked then the identity card cannot be used in that transaction. This raises some questions with regard to the security of the identity card, as well as the possible implications for civil liberties.

Internet fraud

One area of identity fraud which may prove to be the most resistant to the influence of the identity card scheme is fraud on the internet. As discussed in chapter 6, this area of fraudulent activity often involves the use of 'card not present fraud' and techniques of gathering information such as phishing and pharming to enable account takeovers and online false application fraud. While some identity card schemes such as the Estonian National Identity Card system have an online element, the U.K. identity card Bill has not outlined any provision for the identity card to have a virtual presence.

One of the main problems the identity card scheme faces with regard to the internet is that many of the services provided on it are designed in such a way as to not need any face-to-face communication or verification.

Conclusion: what to expect from the identity card scheme

When the new identity card scheme was first proposed in 2002, it could be argued that it was presented as a panacea for several problems. The identity card was presented as a solution to identity fraud, terrorism and illegal immigration. It can be argued that by introducing an identity card the government was trying to put to an end to any and all deception in the identification process. The initial aim of this study was to determine if the identity card scheme would succeed in this goal of stopping identity fraud. But after studying identity fraud and the identity card scheme, it has become apparent that rather than stopping identity fraud the identity card will at most prove to be a new obstacle that must be overcome. By introducing a form of identification where ensuring accuracy is a central concern, the government may be able to create an obstacle to those seeking to commit both identity theft and identity fraud. But it is also important to recognise that the proposed identity card scheme (as it currently stands) still has several significant problems which could degrade its effectiveness as a preventer of identity theft and identity fraud.

Chief amongst these problems is the issue of how the identity card scheme is introduced. According to Home Secretary Jacqui Smith the identity card will rely on consumer demand to drive the uptake of the identity card. It is estimated that the identity card will achieve full coverage of U.K. citizens by 2017. This means that until then the U.K. must by necessity treat the identity card as an optional form of identification for people. If identity thieves wish to avoid the proposed security offered by the identity card they will be able to do so, by claiming not to have an identity card or declaring that they choose not to use it. The identity card can only prevent identity theft and fraud if people are compelled to use it to prove their identity. In terms of security, the identity card can only be seen as solution to identity fraud if it is universally required in the U.K. as proof of identity.

This however raises civil liberties issues which groups such as Liberty, NO2ID and Defy-ID have championed. Looking back at the Second World War identity card, that scheme came to an end because of the mandatory need to present the identity card. If the identity card scheme does rely on consumer demand in its introduction, then it must ensure that the scheme continues to seek the support and acceptance of the general public.

Aside from issues of how the identity card will be introduced and its acceptance by the general public, there are also several questions about how the identity card will work in practice. At present these questions cannot be answered but it is reasonable to assume that issues of security may arise with regard to the following:

- How thoroughly will biographical footprints be checked?

The biographical footprint will be used during applications for identity cards to determine identity. Can this process be fooled by identity thieves? One approach to identity theft and fraud is the use of dead people's identities. With the biographical footprint check, looking at registers of deaths will identity thieves favour targeting the identities of the living rather than the dead?

- How thoroughly will the biometric security be checked?

As discussed earlier, there are several concerns over the efficacy of the biometric security system employed on the identity card. But aside from these concerns there is also the question of how often in practice a person will be required to undergo a biometric check. Additionally, will all three factors – iris scan, fingerprint and facial recognition be used?

- How effective will the identity card be at detecting long term, wholesale and partial assumers?

As shown in the cases of wholesale and partial assumers in chapter 7 some identity thieves spend several years perfecting their impersonations. Will these people modify their activities to adapt to the identity card scheme?

- Will the National Identity Register's Databases be secure from attacks by computer crackers and loss of records?

Recent changes to the identity card scheme have replaced the idea of a single National Identity Register with several databases holding the National Identity Register. This move has been welcomed as it is thought it will reduce the likelihood of the entire register being compromised. But the question still remains as to whether the register is sufficiently protected against abuse by computer crackers. In recent years the security of government databases has been criticised with several high profile losses of public records.

- Will the identity cards be used effectively in the private sector?

Current plans allow for private companies to access the National Identity Register in order to confirm a person's identity. But the degree to which the private sector begins to use and rely on the identity card has yet to be determined.

- Will issues of civil liberty limit the identity cards use?

Arguably while the civil liberty issues surrounding the identity card scheme have not led to it being abandoned, they have influenced the scheme and continue to raise questions

as to the value of introducing the scheme. Both the Conservative and Liberal Democrat parties have declared that if they were in power they would abandon the scheme in favour of other initiatives. It could be that the identity card scheme is abandoned or curtailed significantly long before any benefits from the scheme are experienced.

- What effect will immigration and foreign identification have on the identity card?

One of the first uses of the identity card scheme will be in the identification of immigrants to the U.K. How the identity card application process will operate using identification process from other countries will be an area which will need researching. It can be argued that identification processes from the U.K. would be easier to trust and confirm during the biographical footprint stage. But how much access to foreign databases will there be to confirm immigrants biographical footprints?

As seen in several cases of identity theft and fraud most notably the case of Derek Bond, stealing an identity and using it in another country can be an effective way of concealing identity theft. A situation could arise where a person who commits identity theft in another country could immigrate to the U.K. and use the identity card scheme to validate their impersonation. How the identity card will affect identity fraud in a global context is an important issue to consider and discuss if and when the identity card is introduced.

- How will organised crime respond to the identity card?

Illegal immigration and identity fraud can be very lucrative sources of income for organised crime groups. How organised crime will respond to the identity card will be an important area to study. Will there be attempts to forge or counterfeit the identity card? Will organised crime move away from illegal immigration and identity fraud? Or will they modify their activities to negate the effect of the identity card?

- Will future acts of terrorism change attitudes to the identity card and its powers?

The effectiveness of the identity card in detecting terrorists or terrorist activity has been questioned. Reference is often made to the 2005 bombings in London and the 2007 Glasgow bombing as examples of how an identity card cannot stop terrorism. It has

been argued by some in the government however that the identity card could be a valuable resource in the prevention of terrorism if it can prevent people from using multiple identities.

Looking at the history of the current identity card scheme it can be argued that the terrorist attacks on September 11th 2001 were influential in bringing about proposals for a national identity card scheme. It may be that future developments with regard to terrorism may influence people's attitudes to the identity card scheme and the issue of state surveillance in general. This could result in either further curtailing of the identity card scheme or perhaps an expansion of the scheme.

CHAPTER 10

Overview of Study

Overview of study

This study has focused on two phenomena – the emergence of identity related crimes and the idea of reintroducing an identity card scheme. Since the beginning of the 21st century, concern has risen over the threats of terrorism, illegal immigration and identity fraud. None of these are new crimes, but in the last eight years the profiles of these types of crime have risen dramatically. In response, the idea of reintroducing a national identity card scheme emerged in the U.K. In simple terms, the government sought to solve the problem of deception in identification by hardening the identification process. The question which has formed the basis of this study is whether or not the identity card scheme will succeed in stopping identity fraud. In researching this question, much was learned, not only about the proposed identity card scheme, but about the nature of identity theft and identity fraud. This chapter will provide an overview of three main areas:

- What was learned about identity theft and identity fraud
- Re-starting the Identity Card
- Ongoing developments and future areas of study

In each section of this chapter, there is a brief review, and discussion, of what was discovered.

What was learned from this study?

This study first considered definitions of identity theft and identity fraud. In the U.K., America and Australia, the scope and meaning of the terms identity theft and identity fraud vary. As discussed in chapter 3, some commentators prefer the term identity theft to identity fraud, and vice versa. Some use the terms interchangeably and some use the terms to distinguish between different types of identity related crime. As the definitions of what constitutes identity theft and/or identity fraud are debateable, it is important to review what it means to steal, use or abuse another person's or corporation's identity.

In this study, the history of identity related crime was examined as well as the modern use of the terms identity theft and fraud. It became apparent that while identity theft and identity fraud are modern terms, they refer to well established forms of deception. This study looked back to the 16th century to review the history of deception in criminal activity. In this review of the history of deception, themes of impersonation and misrepresentation emerged with regard to certain acts of identity related crime. Identity theft and identity fraud were distinguished on the grounds of impersonation and misrepresentation. Identity theft was linked to the theme of impersonation. Identity fraud was linked to the theme of misrepresentation. In this way it was possible to distinguish between different activities (cheating individuals versus cheating an institution) and methods of using and abusing the identification process.

Looking at the history of identity theft and identity fraud, it became apparent that both impersonation and misrepresentation can be used to commit crime. Early instances of identity theft tended to be directed at famous people whose identities were well known. Early instances of identity fraud used misrepresentation and deception to trick people into being defrauded.

In the later part of the 20th century and the start of the 21st century, criminals began to use identity theft to enable identity fraud. This shift in the use of identity theft to enable identity fraud is a result of the increased value of people's personal identities. In both the 20th and 21st century, communication technology has improved, allowing people to use their identities quickly over larger distances. The further effects of this are a decrease in the time needed to impersonate someone, and an increase in the opportunities to use and abuse another person's identity

Identity or identification fraud?

During research into simulated identity theft, a question arose about whether or not identity fraud and/or identity theft are actually about identity, as the emphasis in many instances of identity related crime is on the use and abuse of documentation which prove identity.

The role of a person's sense of self in identity theft and identity fraud is something which can be hard to quantify. In some cases of identity related crime, the involvement of the individual's personality or sense of self is extremely limited. For example, the 2003 internet fraud case where a cracker was able to obtain details of five million credit card accounts details from Visa and MasterCard. The cracker was able to break through the security of a company that processed credit card transactions for both businesses. (BBC News, 2003) Apart from cases involving private companies, there have also been several instances of government agencies losing large amounts of data, such as the loss of 25 million child benefit records in 2007; these records included names, addresses, dates of birth, bank details and National Insurance numbers. Either through the theft or the loss of data, it is possible to leave millions of people vulnerable to identity fraud. It can be argued that in these examples, while large numbers of people are being victimised or endangered, there is no interaction with the people's sense of self or their personal identity. Furthermore, what effect can such an incident have on a person's social role, status or personality? Arguably these are far more significant aspects of a person's identity than an account number or a National Insurance number.

There is some merit then to viewing the crimes of identity theft and identity fraud as identification theft and identification fraud. This emphasises that these crimes are about stealing proof of identity, and means that it is easier to focus on the real targets of fraudsters, namely paper proofs of identity, passwords, and personal details.

In most of the cases of modern identity theft considered by this study, there appears to be no real intention to target specifically a particular person. The exception to this has been cases of identity theft within families. However, aside from these cases, many of the victims described in this study have been victims of circumstance. Through the use of gathering and appropriating techniques some people have found themselves vulnerable to attack. A good analogy would be a fisherman trawling for fish with a net. With recognition of the practice of identity theft via the internet, this analogy has lead to the use of the term phishing to describe how fraudsters use e-mails to steal money. The

analogy, however, holds true for many forms of data gathering used by identity fraudsters.

Thus, there is some value in interpreting identity related crime as the theft and abuse of proofs of identification, rather than the theft and abuse of a person's identity. Certainly, in cases of identity related crime involving illegal immigrants and terrorists the focus is on the abuse of identification rather than abuse of a specific person's identity. However, it can also be argued that the alternative position, focusing on identity theft and identity fraud as abuses of a person's sense of self, also has merit. Modern cases of identity theft and identity fraud are often much quicker and easier to commit than in previous centuries. Nevertheless, this does not mean that the sense of victimisation felt by people who have their identities stolen is overcome just as quickly. It can be argued that the sense of abuse felt by modern victims of identity theft is only magnified by the speed at which some identity thieves can steal a person's identity.

The role of victims in identity theft and fraud has been an important factor in raising the profile of identity related crime. It can be argued that it was the protests of victims such as Michelle Brown or Derek Bond (see pages 109 and 113) that raised public awareness and concern over identity related crime. Both in America and the U.K., the experiences of victims of identity related crime have compelled governments to introduce new legislation. In America, the experiences of Michelle Brown led to the introduction of identity theft laws. Equally, the introduction of an identity card scheme is in part due to public concern over becoming a victim of identity fraud. While fraud has often been viewed as a victimless crime, the recent media attention given to victims of identity theft has undermined this idea.

The accounts of victims' experiences are also a useful source of information on how an identity can be abused by criminals. Reports given to victim support and advocacy groups such as the Privacy Rights Clearing House and the Credit Industry Fraud Avoidance System as well as media reports highlight new developments in identity related crime. As society develops, along with new and more elaborate uses for people's

personal identities, new forms of identity related crime may emerge. Only by monitoring new developments in the experiences of identity theft and fraud victims can criminology, the National Identity Card Scheme and the state in general, hope to keep pace with the ways in which identity can be abused.

The study of victims of identity theft also reveals the importance of social trust in society. This study has argued that a key element of identity related crime is the abuse of bonds of trust, most notably social trust. In many aspects of life, there is a dependence on social trust to enable a variety of different social interactions. It is the assumption that people will be truthful about who they are which identity thieves depend upon. The numerous cases of identity theft discussed in this study have all, in some way, depended on people assuming at some point that the criminal can be trusted.

If social trust were curtailed in favour of increased security and surveillance, it could mean an improvement in protection against identity theft. By increasing security around the identification process, there would be less dependency on social trust. The identity card scheme is, in a sense, a way of replacing social trust in strangers with a state guarantee. If there are instances of identity theft or fraud, the identity card can also be used as a means of state surveillance to track and detect deception.

It can be argued that replacing social trust with increased security and surveillance is a good thing for combating identity theft. However, by decreasing social trust between individuals within society, an indirect effect could be a decrease in social trust between the state and the general public. The threat of losing social trust between the state and the general public was the reason the last identity card scheme was abandoned in 1953. Fear over the abuse of surveillance technology by the state is essentially an issue of social trust.

Do we as a society continue to trust that strangers will tell the truth about who they are (social trust)? Or do we increase the use of surveillance and security in the identification process, stop trusting people to tell the truth and instead make sure that no one can lie? As Barry Steinhardt said:

> "There is no longer a technological barrier to a surveillance society." (Steinhardt .B, 2004: 1)

If there is no longer a technological barrier to a surveillance society, then the debate over increasing surveillance becomes an issue of how much social trust there should be in society. In terms of identity theft and fraud, it can be argued that these crimes are an abuse of social trust so the less society relies on social trust, the safer people will be from these types of crime. However replacing social trust with increased security and surveillance in the identification process poses its own threats to civil liberties.

Criminal liability and identity theft and fraud

The experiences of those whose identities were used to avoid criminal liability also undermines the idea that identity theft or fraud is only about identification and proof of identity. For instance the experiences and harm felt by Dr Grout and Michelle Brown after being held responsible for the actions of their identity thieves.

The issue of whether or not identity related crime is an attack on a person's identity or an abuse of identification was in part raised during the simulation of identity theft discussed in chapter 5. In the simulated identity theft thought experiment the effect simulated identity theft might have on the donor identity provided by the research subject was considered. It was determined that the risk posed to the research subject's sense of self and potential harm to their relationship with society made the simulation unethical. Furthermore, there was a sense that the proposed simulation also failed to accurately portray identity theft. The targeting of one person specifically did not display the manner in which identity fraudsters might trawl for information on anyone who is vulnerable to attack.

These two issues are important to consider in the future, as focusing on one approach or the other will influence how we treat and respond to identity related crime. Treating identity theft or identity fraud as if these were only an abuse of proofs of identity may help in the policing of these crimes. Identity frauds committed by online criminals, for instance, have often focused on the abuse of certain forms of identification. For the most part, the efforts have not been to persecute individuals specifically, but to exploit access to proofs of identity. The emphasis for criminals is on the identification more so than on the identities. So in investigating identity related crime perhaps focusing on identification may also help.

However, it is also important to acknowledge the experiences of victims of modern identity theft and fraud, and the sense of abuse of social trust. The experiences of victims of identity theft and fraud have motivated a change in the public perception of fraud as a victimless crime. It can be argued that if people did not feel a threat to their personal identity or to the identification process in general, then calls for the introduction of an identity card scheme would not have emerged.

Criminality of false representation

Another area researched in this study is the criminality of false representation. Prior to researching the law on representation it was assumed that there was a degree of legal ambiguity in relation to lying about who one is. However, recent developments in the law with regard to fraud have sought to criminalise false representation. This change in the law, in conjunction with new legislation against forgery and the theft of identifying documentation, has placed more of an emphasis on identity related crime and its illegality.

Although strengthening the law should provide more power to prosecute those who use false representation, there is still the issue of how much of a priority identity related crime is for the police, and how easy or difficult it is to prosecute. Looking at the American and their identity theft laws, commentators such as Sullivan (2004) have

argued that while there is a law prohibiting identity theft, the complexity of the law and the time it takes to investigate identity theft, means prosecution is still difficult. Of the U.K. cases researched in this study, the majority of prosecutions discussed involve large scale crimes, often with large numbers of victims or great amounts of money taken. Cases involving identity fraud to avoid criminal prosecution are an exception to this, but in these instances there has often been a lot of media attention.

How much attention or effort is given to individual cases of false application, fraud, or account takeover, is an area which requires further study. CIFAS surveys and reports from 1999 to 2007 suggested that there had been a sharp rise in the levels of identity fraud and victims in the U.K. While these figures are open to interpretation and scrutiny, they would nevertheless suggest that there are a number of identity fraud cases which actually receive very little media attention. The way that these victims and their cases are dealt with by the police will provide a degree of insight into the value of new legislation on false representation.

Re-starting the identity card scheme

With regard to the identity card scheme, this study found that the first major obstacle this scheme would face was its reintroduction. As the card is not the first form of identification a person will have in the U.K., the manner in which the scheme is introduced will be a vital aspect of the card's potential as a secure form of identification. The identity card is in effect being grafted on to a pre-existing system of identification. In order to identify people, the scheme is forced to rely on information about them gained from other proofs of identity. Since the identity card is also being introduced because of the lack of security in these other forms of identification, how applications for the identity card are handled will be a crucial issue. When discussing the identity card scheme, the government have been vocal on the security it will provide through the use of biometrics. But the biometric security system will only come into effect when the system is already in operation. Before it reaches the point where biometric security comes into effect, the identity card must go through a period of setup and application. During this period, the identity card must deal with the problem of false application by

relying on biographical foot-printing, and on previously established proofs of identity. This situation creates a strange paradox: in order effect this 'secure' form of identification, it has to rely on the very forms of identification it is aimed to replace.

False application and biographical footprints

Before the identity card scheme can be considered a secure form of identification, it must establish itself as an accurate identifier. In order to do that, it must first of all ensure that everyone who applies is who they say they are. The way the scheme will do this is by checking on the past history of applicants in order to establish the applicant's biographical footprint. That the identity card scheme must establish its identification of people through the use of other forms of identification raises questions over its potential to be accurate at this first stage.

Ideally, if the identity card could come in as the first form of identification a person ever receives in their life, then it could guarantee that there is no doubt as to who is applying for it. By being first form of identification and autonomous from all other forms of identification, the identity card could be a truly secure form of identification, providing an unbiased view of people's identities. As the system stands now, it will not be the first form of identification a person gains in their life. As a consequence, there is an opportunity for impostors to apply for an identity card under an assumed name. Provided they can apply for the card first, and beat the biographical footprint check. Research conducted during this study has shown how identity thieves can gather enough information about someone to achieve a successful impersonation, using current proofs of identification. If the biographical footprint check is not thorough then it maybe that identity cards will fail in their first task, namely accurately identifying who is who in the U.K.

This issue of making sure that legitimate identity holders obtain their identity cards is an important one. As there is a prolonged introduction process for the identity card scheme, it is possible that identity thieves may try to obtain identity cards before the legitimate identity holders get around to applying for their identity cards. The value in applying for

another person's identity card is debateable. By providing their biometrics (including a picture of themselves) the identity thieves would be risking a great deal. It would also mean the identity thief could not apply for another identity card. In effect, this would prevent them from using more than one other person's identity card. In order to obtain multiple identity cards, in different names, the identity thief would have to gain access to the National Identity Register and alter the data held there.

There are situations where obtaining only one other person's identity card would be necessary or desirable for the identity thief. In instances of wholesale assumption, people will only want to establish one alternative identity. It may be that illegal immigrants or terrorists only require one alternative identity and will seek to validate that alternative identity as much as possible. Equally, identity thieves may falsely apply for an identity card in order to use it as a proof of identity in other countries. Identity thieves may also obtain identity cards in order to use them in parts of the private sector that do not or cannot access the National Identity Register.

The thoroughness of the biographical footprint check for identity cards is important to ensure that the identity cards are issued to the legitimate identity holders. Even if the identity card scheme fails to ensure that there are no cases of false application, it should ensure that identity thieves have difficulty using multiple identities.

Multiple identities

Ideally, what the identity card scheme must be able to do, is to prevent the use of multiple identities. Using biometrics to ensure that one person's biology is linked to only one identity, would mean that fraudsters could not steal or use another person's identity in the U.K. If the identity card scheme is also linked into an e-passport scheme, it would mean that travel and use of multiple identities abroad could also be curtailed.

If the identity card can stop the use of multiple identities then it would mean that several forms of identity fraud could be prevented. False application, account takeover, and the

use of identity fraud to avoid criminal liability could be stopped. The only aspect of identity fraud which might continue to occur would be wholesale assumption.

Account takeover and biometric security

Apart from issues of false application, the other area where the identity card scheme may face difficulty is those occasions where criminals attempt to takeover and use someone else's identity card. The use of biometric security should prove to be an obstacle to those trying to takeover someone else's identity card. This would only be true as long as there are no problems that might arise with regard to failure to read a person's biometrics, for instance problems with the calibration of biometric readers or damage to a person's fingerprints, iris' and/or face. In principle, the biometric security system should ensure that any attempt to use another person's identity card will fail, as it is statistically highly unlikely that two people have the same biometric measurements. The danger of account takeover, with regard to the identity card scheme, depends on how often the identity card can be used without the biometrics being checked. If a situation arises where the identity card is accepted as proof of identity without checking the biometrics, then it may be possible for people to steal and use other peoples' identity cards. This situation may occur if and when the identity card is used in the private sector where access to the National Identity Register may be limited. Alternatively it may be that biometric scans are taken on a regular basis as part of the identification process. This would ensure the early detection of someone trying to use another person's identity card. However, repeated checking and monitoring of people's biometrics also has implications with regard to the increase in state surveillance.

Time until full coverage

As stated in chapter 9, estimates of how long it will take until everyone in the U.K. has an identity card, put full coverage of the identity card scheme by 2017. This means that until then people will be able to identify themselves without the need for an identity card. Consequently there will still be value in stealing and abusing forms of identification such as drivers' licences, passports and National Insurance numbers. It

also means people will still be able to apply for bank accounts and credit cards without using an identity card.

If not Identity Cards then what?

It has been recognised in this study that the idea of introducing an identity card scheme is a contentious issue. Opposition to the identity card is based on its impact with regard to civil liberties and the increase in the use of surveillance technology by the state. Political opponents have also criticised the identity card on the grounds of cost. With decision of whether or not the identity card scheme will develop or not being a highly politicised issue, it is worth considering what possible alternatives there may be to an identity card scheme. While both the Conservative party and the Liberal Democrats have declared their opposition to the identity card their stance on combating identity fraud is harder to discern.

Both the Conservative and Liberal Democrat parties have given examples of what they would do with the money they would save by not introducing the identity card. Both parties championed the idea of a National Border Agency to tackle illegal immigration, and in April 2008 this agency took over the responsibility for border security from several government agencies. The Liberal Democrats have also put forward the idea of using the money saved by not introducing the identity card scheme to recruit 10,000 additional police officers. However, as stated in chapter 4, there is still no clear idea of how the Conservatives or the Liberal Democrats would combat identity fraud if they came to power. The emphasis has been on targeting terrorism and illegal immigration. These are important issues to address, but there are still questions as to how financially motivated identity fraud, of the type discussed in chapter 8, will be combated.

Possible initiatives to stop identity fraud

Given below are several possible approaches to combating identity fraud, which could be used either as an alternative to the identity card or used in conjunction with it. These ideas seek to address the areas of identity related crime which the identity card scheme may not succeed in preventing or detecting.

1. Virtual Wallets

One of the dangers faced by users of the internet is that access is gained to their bank accounts or credit cards and their accounts are taken over (see chapter 8 for account takeover). The loss of account details is always a threat because when someone is making transactions on the internet, there is the possibility that information is being communicated to a third party. This is a threat with any transaction including non-internet based transactions. So if the security of the account details cannot be ensured, the next best thing is to ensure that the account details do not lead to access to a great deal of money or information.

A virtual wallet would be similar to a real wallet, if a wallet is lost or stolen then it is possible to limit the effects of that loss by shutting down the accounts, reporting the cards stolen, etc. A virtual wallet would be a credit or debit account specifically intended for use on the internet. Limits both on the credit limit on the account, and perhaps on where it could be used on the internet could ensure a limit on the amount of damage that could be done if the account details were stolen.

One fraud that is used on the internet is to steal someone's account information and then use it to finance online gambling. If people were encouraged to create an account that is used exclusively on the internet, then certain types of websites could be excluded. For instance if someone tries to use the account to access gambling or pornography, billing from these accounts could be blocked.

Most security efforts on the internet are designed to secure the individual websites from crackers, especially since frauds such as phishing and pharming have shown how the requisite information can be obtained to challenge this security, and there is a number of websites that do not scrutinise security as effectively as is necessary. It is important that individuals are better protected from online fraudsters. If online fraud cannot be stopped

or security cannot be ensured, then individual customers must be given a means of protecting themselves from the risks posed by using the internet.

2. Shredding Watermarks

In chapter 7 the use of bin-raiding as a means of gathering information is discussed. One possible solution to the threat posed by bin-raiding would be to inform people if a document holds any identity sensitive information. A shredding watermark or symbol could be added to documents indicating that they must be destroyed before discarding. If this watermark were a standardised requirement, it could help to inform the general public as to the threat posed by identity thieves. A shredding watermark would also help to inform organisations which handle identity sensitive documents and information.

3. Less speed more security

As noted earlier, the simple fact that people are used to quick service directly affects the provision of security. In order to avoid the dangers posed by identity fraud, the simplest and possibly the hardest thing to do, would be to require more security checks and a reinforcement of pre-existing security checks to ensure accuracy. This would require more of a cultural change as much as anything - no more instant credit, no more online transactions. It is unlikely that this would happen, but awareness that doing things quickly may be dangerous might help inform people. The issue of speed versus security is an important factor with regard to the identity card scheme. As has been noted, the introduction of the identity card will require an application process where people's biographical footprints are checked. The time taken to check a person's biographical footprint will affect the likelihood of a false application succeeding. The more time is taken to thoroughly check someone's biographical footprint, the better, in one sense. However, the longer the application process takes the more time it will take before the identity card can become a universal form of secure identification.

4. More effort in catching online criminals

As a result of the international nature of the internet, it is possible for criminals in one country to steal from people in another. Online fraud gangs do not have to worry about

national borders and because of holes in internet security there is little that can be done to catch them in the commission of their crimes. During discussion with Mrs B and her experience as a victim of identity theft, the police noted that the likelihood of capturing or ensuring a conviction for this type of crime is next to zero. The sense that these crimes (and the people who commit them) are in some way unstoppable, may be true. If there were an increase in international efforts to detect and prosecute online criminals, it might be possible to have a more significant impact on this type of crime. However, there are countries such as Russia and China where the influence of organised crime may impede efforts to investigate online identity fraud.

5. Fraud Awareness

It can be argued that the emergence of identity fraud as a phenomenon of the 21st century is in a way a form of moral panic over a crime that has always been a problem (see chapter 6 for history of identity related crime). But while the dangers individuals face from being unprepared are well known through the accounts of Derek Bond and Michelle Brown, the actual methods of protecting oneself are underreported, as are the resources available to victims of this type of crime.

6. Security against internal collusion

In many respects, the responsibility for protecting an identity lies with the individual, but equally individuals are dependant on the organisations they interact with and share information with to keep this information safe. There have been several instances (see chapter 7) where individuals in the employ of organisations have sold information about people's identities. The security surrounding call centres and individuals who are responsible for handling 'identity sensitive' information is one area which needs more attention.

With the introduction of the National Identity Card Scheme and the National Register the issue of internal collusion with corrupt officials will become even more important. The individuals placed in charge of inputting information to the register will have the opportunity to steal this information. Moreover, there is also concern about corrupt

members of organisations inputting false information or altered information, in order to create new or alternative identities for those seeking to change their identity.

7. Card not present fraud

One form of identity fraud which will not be directly affected by the introduction of the National Identity Card Scheme is Card Not Present Fraud (CNPF). This is the type of fraud committed on the internet and through any transaction where there is no direct contact between the seller and the purchaser. According to the Association for Payment Clearing Services (APACS) in their 2007 report – *'Fraud The Facts'*, CNPF cost the U.K £212.6 million in 2006, a 74% rise from 2003. This type of fraud is highly resistant to any protection offered by the National Identity Card Scheme, as this type of crime requires no contact where an identity card may be used fully.

Ongoing developments and future areas for study

The aim of this study has been to outline the 'potential' effect of the National Identity Card scheme on identity fraud: it was necessary to consider how identity fraud is committed before the introduction of an identity card scheme, and then to determine what an identity card scheme might do.

The next step, after this study, is to see what happens when the identity card scheme begins. The next issues to address will concern how applications for the identity card are handled, how the biographical footprint checks work, and how the biometric security system works in preventing identity fraud. Additionally, the following areas of research should be addressed:

1. Further research into simulated identity theft

As discussed in chapter 5, Simulated Identity Theft was considered and ultimately abandoned as a research method. While the ethical issues associated with this research method are difficult to resolve, further study of the use of simulated identity theft as a hypothetical process for assessing how identity theft may occur could be useful. While going forward to commit simulated identity theft is not advisable, the planning process

can help researchers to consider how the identification process can be abused, and the relative value and significance of different forms of identification. Further research into how to simulate identity theft would be useful to maintain an understanding of how identity theft and fraud is committed. Interviews with those who have used simulated identity theft, for example investigators from the General Accounting Office would be useful in any future research into simulated identity theft.

2. Study of information gathering, both legal and illegal (data searches and bin-raiding)

An area which also needs further research is the process of obtaining information on people. Further research into both legal and illegal methods of gathering information will help to improve our understanding of how people's identities are obtained and used. In this study, it has been argued that the illegal gathering of information on people can speed up the process of committing identity theft. Therefore, it is important to seek out and research new developments with regard to illegal approaches of obtaining information used by identity thieves.

The other area of gathering information on people which warrants more research is the legal gathering of information. An area of legal information gathering which has not been explored in this study is the harvesting of information by large corporations. Data harvesting is a practice of gathering information on people for the purpose of market research and targeting of people for the sale of certain products. This process can result in large amounts of information being gathered on people's identities. How information is used, and perhaps even abused, is an area which requires more research.

3. Illegal immigration and identity fraud as a multinational problem

Further research on the use of counterfeit and forged documents by people smugglers is important. An area of particular importance with regard to identity fraud and people smuggling is the use of forged or stolen identification to cross national borders. As discussed in chapter 3, there have been some journalistic investigations into the use of false passports and identification by illegal immigrants. Nevertheless, further research

into this topic and the role and effect of the new e-passport and/or U.K. identity card scheme may be beneficial.

It would also be valuable to investigate identity theft and identity fraud as a multi-national problem; this would provide a means of assessing the influence the National Identity Card Scheme may have when it is used as proof of identity abroad. It could be that the identity card becomes a secure form of identification which prevents identity theft in the U.K., but is easily abused in other countries. Looking at the case of Derek Bond whose identity was misused in America for over 20 years, it is clear that committing identity theft and/or identity fraud over national borders can help to obscure and prolong impersonations and misrepresentations.

4. Better understanding of the role of the internet

It has been argued in this study that fraud on the internet is an area where the identity card scheme will have little effect. The use of the internet to enable identity theft is something that requires more attention, as is the use of computer software to steal information on people.

Final Statement

The question which has formed the basis of this study is whether or not the identity card scheme will succeed in stopping identity fraud. This study argues that identity theft and identity fraud are complex forms of criminal activity, which the identity card scheme will struggle to eliminate completely. What the identity card scheme must endeavour to do is to accurately identify people, removing as much deception from the identification process as possible. It must seek to prevent people from using multiple identities. If the scheme succeeds, it is foreseeable that it will curtail identity fraud involving the public sector. Its influence on private sector fraud will depend on the popularity of non-face-to-face interactions (e.g. the internet) and the uptake of the scheme by private companies. The identity card will be a new way to combat identity theft and fraud but it will not be a solution to the entire problem.

CHAPTER 11
BIBLIOGRAPHY

Anon, (2006), *Social Engineering 101*, Social Engineering forum for Social Engineers SE http://www.socialengineering101.com/viewforum.php?f=3 viewed 3/03/07

Aaron .B, (May 15 2007) *How Not To Lose Your Identity*, Channel 4

Abagnale .F.W, Redding .S, (2003) *Catch Me If You Can*, London, Mainstream Publishing

Abercrombie .N, Hill .S Turner .B.S, (1988), *Dictionary of Sociology, 2nd Edition*, London, Penguin Books.

Airey .S, Cooper .K, (2006), *Stop Thief!*, Rexel News Release, page 1

Ali .J, (2004), *UK 'not ready' for ID card scheme*, BBC News, http://news.bbc.co.uk/go/pr/fr/-/1/sci/tech/3933319.stm viewed 05/11/04

Allison .R, (February 28 2003 pg 2), *Conman who stole Bonds identity named as Briton*, Guardian, http://guardian.chadwyck.co.uk/noframes/quick/fulltext?ACTION=... Viewed 25/10/04

Ampratwum .E.F, (2009), Advance fee fraud "419" and investor confidence in the economies of sub-Saharan African (SSA), *Journal of Financial Crime*, vol 16, Issue 1, pages 67 - 79

Amos .J, (2005), *Criminals to 'adapt to ID cards'*, BBC News, http://news.bbc.co.uk/1/hi/sci/tech/4213848.stm viewed 22/09/08

Anderson .R, Brown .I, Dowty .T, Inglesant .P, Heath .W, Sasse .A, (2009), *Database State,* Joseph Rowntree Reform Trust Ltd, http://www.jrrt.org.uk/uploads/database-state.pdf viewed 17/08/09

aNewidentity.com, (2007) *Your Future is Waiting*, http://www.anewidentity.com/ viewed 5/6/07

aNewidentity.com, (2007) *Advantages of A New Identity, Inc.*, http://www.anewidentity.com/advantages.htm viewed 5/6/07

Ariza-research.com, (1995), *Change your identity*, http://www.ariza –research.com/new-id/ viewed 06/10/04

Association for Payment Clearing Services, (April 26 2002), *Unique Police Unit Pilot to Hit Organised Card Crime,* http://www.dcpcu.org.uk/HTML/launch.html viewed 23/09/08

Association for Payment Clearing Services, (2007), *'Fraud The Facts'*, http://www.apacs.org.uk/resources_publications/documents/FraudtheFacts2007.pdf viewed 18/09/08

Australian Centre Policing Research, (May 2004), *Standardising ID crime Australia,* http://www.acpr.gov.au/publications.asp viewed 22/03/06

Bangor News (2005), *Woman pleads guilty to id theft*, Bangor Publishing Company, http://www.bangornews.com/news/templates/default.aspx?a=12192... Viewed 14/10/2005

Bashir .M, Wallace .R, (2006), *Fake English Lord's Identity Revealed Charles Buckingham's Web of Deceit Unravels After Two Decades,* ABC News, http://abcnews.go.com/Primetime/story?id=2173695&page=1 viewed 27/08/09

BBC News Online, (September 8 1998) *Fake who wrecked lives and justice,* http://news.bbc.co.uk/1/low/uk/167174.stm viewed 14/11/2006

BBC News Online, (July 19 1999), *UK Stealing Identities,* http://news.bbc.co.uk/1/hi/uk/398455.stm viewed 07/11/2006

BBC News Online, (2002), *FBI busts identity theft ring,* http://news.bbc.co.uk/1/low/business/2513015.stm Viewed 22/05/05

BBC News Online, (April 4 2003), *Police offer to shred papers,* http://news.bbc.co.uk/1/hi/england/2915853.stm viewed 29/06/07

BBC News Online, (February 18 2003), *Credit card database hacked,* http://news.bbc.co.uk/go/pr/fr/-/1/hi/business/2774477.stm viewed 07/11/2006

BBC News Online, (2003), *Gang jailed for people smuggling,* http://news.bbc.co.uk/go/pr/fr/-/1/hi/england/west_midlands/3284957.stm viewed 22/09/08

BBC News Online, (2004), *'Ignorance' over identity theft,* http://news.bbc.co.uk/go/pr/fr/-/1/hi/uk/3754106.stm viewed 22/05/05

BBC News Yorkshire & Lincolnshire, (October 4, 2004), *Invisible Predator, Inside Out,* http://www.bbc.co.uk/insideout/yorkslincs/series6/computer_doctor.... viewed 14/05/2007

BBC News Online, (October 22 2004), *Warning over rubbish bag slashers,* http://news.bbc.co.uk/1/hi/england/tees/3944033.stm viewed 22/09/08

BBC News Online, (April 21 2004) *Doctor acquitted of porn charges*, http://news.bbc.co.uk/go/pr/-/1/hi/england/humber/3647207.stm viewed 14/05/2007

BBC News Online, (October 21 2004), *Doubts over passport face scans*, http://news.bbc.co.uk/1/hi/uk/3762398.stm viewed 15/05/2007

BBC News Online, (2005), *Postman is jailed for £20m fraud*, http://news.bbc.co.uk/1/hi/england/london/4555174.stm viewed 22/09/08

BBC News Online, (June 26 2005), *ID card database 'not for sale'*, http://news.bbc.co.uk/1/hi/uk_politics/4624735.stm viewed 1/07/07

BBC News Online, (June 30 2005), *Illegal immigrant figure revealed*, http://news.bbc.co.uk/1/hi/uk_politics/4637273.stm viewed 10/07/07

BBC News Online, (October 24 2006), *Three Jailed for Identity Thefts*, http://news.bbc.co.uk/go/pr/fr/-/1/hi/england/london/6079390.stm viewed 07/11/06

BBC News Online, (May 10 2007), *Child porn suspects blame fraud*, http://news.bbc.co.uk/go/pr/fr/-/1/hi/uk/6641321.stm viewed 14/05/2007

BBC News Online, (March 20 2007), *10,000 passports go to fraudsters*, http://news.bbc.co.uk/1/hi/uk_politics/6470179.stm viewed 10/07/07

BBC News Online, (February 23 2007), *1,000 passports 'missing in post'*, http://news.bbc.co.uk/1/hi/uk_politics/6387925.stm viewed 10/07/07

BBC News Online, (February 22 2007), *Fraudulent forensic expert jailed*, http://news.bbc.co.uk/1/hi/england/manchester/6386069.stm viewed 20/08/09

BBC News Online, (2008) *Rethink on identity cards plans*,

http://news.bbc.co.uk/go/pr/fr/-/1/hi/uk_politics/7280495.stm viewed 11/8/08

BBC News Online, (2008) *Secret Life of Fugitive Karadzic*, http://news.bbc.co.uk/1/hi/world/europe/7520661.stm viewed 20/01/09

Beare .M.E, (1999), Illegal Migration: Personal Tragedies, Social Problems, or National Security Threats? in William P, (ed.1999), *Illegal immigration and commercial sex: the new slave trade,* London, Frank Cass

Bearman .R, (2004), *A Guide to Social Engineering*, BastardOps.net, ross@bastardops.net viewed 22/09/08

Beck .U, Beck-Gernsheim .E, (2001), *Individualization*, Sage, London

Bell .R, (2006a) *Treva Throneberry: A Nightmarish Youth*, Court TV Crime Library http://www.trutv.com/library/crime/criminal_mind/scams/treva_throneberry/2.html viewed 08/03/2006

Bell .R, (2006b) *Treva Throneberry: The Girl Who Refused to Grow Up*, Court TV Crime Library, http://www.trutv.com/library/crime/criminal_mind/scams/treva_throneberry/ viewed 8/03/06

Berinato .S, (2007), *Who's stealing your passwords? Global hackers create a new online crime economy*, cio.com, http://www.cio.com/article/print/135500 viewed 19/06/2008

Better Business Bureau, (2005), *Victims Stories*, BBB Online, http://www.bbbonline.org/idtheft/stories.asp viewed 11/09/08

Bird .S, Browne .C, (2005) *Tsunami victims' identities are under threat from gangs*, The Times Online, http://www.timesonline.co.uk/tol/news/world/article416140.ece viewed 23/07/08

Boggan .S, (August 6 2008), *'Fakeproof' e-passport is cloned in minutes*, The Times, timesonline.co.uk viewed 22/09/08

Brown .M, (July 2000), *Written Testimony of Michelle Brown*, Privacy Rights Clearinghouse, http://www.privacyrights.org/cases/victim8.htm viewed 27/03/06

Bruce .S, (August 30 2007), *£250,000 fraudster stole sister's life*, thisismoney.co.uk, http://www.thisismoney.co.uk/news/article.html?in_article_id=423823&in_page_id=2 viewed 09/05/2008

Bulow .L, (2008), *Josef Mengele*, The Holocaust Crimes, Heroes and Villains, http://www.mengele.dk/new_page_2.htm viewed 29/07/09

Burton .S, (2000), *Impostors: Six kinds of liar*, Harmondsworth, Penguin Books

Butcher .M, (April 27 2003), *Crime Uncovered: IT BYTES: THEY'VE GOT YOUR NUMBER*, The Observer,
http://guardian.chadwyck.co.uk/noframes/quick/fulltext?ACTION=...
Viewed 25/10/04

Caldwell .G, Galster .S, Kanics .J, Steinzor .N, (1999), Capitalising on Transition Economics: The Role of the Russian Mafiya in Trafficking Women for Forced Prostitution in Williams .P (eds 1999), *Illegal Immigration and Commercial Sex: The New Slave Trade,* London, Frank Cass Publishers

Campana .J, (2006), *Identity Theft: The Business Time Bomb*, J. Campana & Associates, http://download.101com.com/pub/spo/files/BusinessTimeBombWhitePaper.pdf viewed 29/04/09

Career Builder India, (2007) *Is Your C.V. a Lie?,* CareerBuilder.com. http://www.careerbuilder.co.in/in/jobseeker/careeradvice/viewarticle.aspx?articleid=11&cbRecursionCnt=1&cbsid=41cb64dc5d5a4b3c8c7059be223c48a1-270723377-VA-4&ns_siteid=ns_uk_y_Lying_C.V viewed 30/7/08

Carroll .R, (2005), *Cold Reading*, The Skeptics Dictionary, http://skepdic.com/coldread.html viewed 01/09/08

Chakrabarti .S, (2007), *Yet Another Step Along a Dangerous Road*, Liberty, http://www.liberty-human-rights.org.uk/publications/pdfs/privacy-indie-scjan07.pdf viewed 12/04/08

Chwala .S, Pietschmann .T, (2005), *Trafficking in Human Beings and Smuggling of Migrants*, in Reichel .P, (ed. 2005) *Handbook of transnational crime & justice*, Thousand Oaks, Sage Publications

Conservative Party, (2007), *ID cards: Labour's bad idea*, Conservative party website, http://www.conservatives.com/title.do?def=campaigns.display.page&obj_id=134894 viewed 05/07/07

Crary .D, (2003), *Passing for white*, South Florida Sun Sentinel, http://www.racematters.org/passingforwhite.htm viewed 20/01/09

Credit Industry Fraud Avoidance System, (2007) *Is Identity Theft Serious?*, CIFAS Online, http:www.cifas.org.uk/default.asp?edit_id=556-56 viewed 01/09/06

Credit Industry Fraud Avoidance System, (2004), *How Serious Is The Problem?* CIFAS Online,
http://www.cifas.org.uk/identity_fraud_is_theft_serious.asp
viewed 09/12/04

Credit Industry Fraud Avoidance System, (2008), *Impersonation of the Deceased*, CIFAS Online, http://www.cifas.org.uk/default.asp?edit_id=555-56#Impersonation_of_the_Deceased viewed 24/02/09

Crichton .R, (1959), *The Great Impostor the amazing careers of F.W.Demara* , New York, Random House reprinted in 2001 by AnEx Publications
http://www.anexx.com/AnEx/greatimpostor/ viewed 12/09/08

Curwen .L, (August 7 2006), *It's a Steal: ID Theft*, BBC News,
http://news.bbc.co.uk/go/pr/fr/-/1/hi/programmes/inside_money/5203580.stm viewed 07/11/06

Davies .S, (August 24 1996), *Identity Cards, Frequently Asked Questions*, Privacy International,
http://www.privacy.org/pi/activities/idcard/idcard_faq.html
Viewed 12/12/2003

Davies .S, (October 31 2004), *Do you want MI5 to know your medical details? They soon will - and it will cost you £35*, Mail on Sunday,
http://www.mailonsunday.co.uk/home/search.html?searchPhrase=Do+you+want+MI5+to+know+your+medical+details%3F+They+soon+will+-+and+it+will+cost+you+%A335 viewed 27/08/09

Defy-ID, (2004-05), *New Suit, Same S*it*, Defy-ID Winter Bulletin, www.defy-id.org.uk viewed 27/07/07

Detica (2005) *Personal information: on sale at a call centre near you*, Detica Information Intelligence, http://www.detica.com/indexed/Opinion_callcentreidtheft.htm viewed 3/10/2005

Durkheim .E, (1964), *The division of labor in society. Translated by George Simpson* , New York, Free Press of Glencoe

Eldridge R.T, Ginsburg S, Hempel W.T, Kephart J.L, Moore K, (2004), *9/11 and Terrorist Travel,* Staff Report of the National Commission on Terrorist Attacks upon the United States, http://www.9-11commission.gov/staff_statements/911_TerrTrav_Monograph.pdf viewed 24/07/09

Engbersen .G, Van Der Leun .J, (2001), The Social Construction of Illegality and Criminality, *European Journal on Criminal Policy and Research,* vol 9 no 1 51-70

ESRC Identities Programme, (2003), *Identities and Social Action: a Programme Proposal*, Open University, www.esrc.ac.uk/.../**Identities**%20and%20**Action**%20Specification_tcm6-5892.doc viewed 26/06/09

Europol, (February 2008), *Trafficking in Human Beings in the European Union,* http://www.europol.europa.eu/index.asp?page=publications&language= viewed 15/05/09

Europol, (March 2008), Facilitated Illegal Immigration into the European Union, http://www.europol.europa.eu/publications/Serious_Crime_Overviews/Facilitated_illegal_immigration_2008.pdf viewed 15/05/09

Experian, (2005), *Lifting the lid off identity theft and transaction fraud,* CrediNews April 2005, http://www.experian-scorex.com/Web/News/Newsletters/e-news-SAfrica_05-04.pdf viewed 23/09/08

Federal Bureau of Investigation, (2005) *Busted for Katrina Fraud: The Case of the Phony Pilot*, F.B.I, http://www.fbi.gov/page2/oct05/katrinaescam102105.htm viewed 17/07/08

Feather .F, (2007), *LIVING a "WEB LIFESTYLE"*, FutureTrends.com http://www.future-trends.com/weblifestyles.html viewed 8/09/08

Federal Trade Commission, (1998), *Identity Theft and Assumption Deterrence Act*, http://www.ftc.gov/os/statutes/itada/itadact.htm#003 viewed 22/09/08

Fickling .D, (2004), *'Mossad spies jailed over New Zealand passport fraud*, The Guardian, 16th July pg 18,

Financial Supervision Commission, (2008), *News Release PUBLIC WARNING FALSE IDENTITY DOCUMENTS Camouflage and Fantasy Passports*, http://www.gov.im/infocentre/archived_releases/PR_fsc_01/Passport.html viewed 22/09/08

Finch .E, (2003) 'What a tangled web we weave: identity theft and the internet', in Jewkes .Y, (eds 2003) *Dot.con: Crime, Deviance and Identity on the Internet*, Collumpton, Willan Publishing

Finckenauer .J, Albanese .J, (2005), Organised Crime in North America, in Reichel .P, (eds. 2005) *Handbook of transnational crime & justice*, Thousand Oaks, Sage Publications

Fraud Advisory Panel, (2003), *Identity Theft: Do you know the signs?*, Crime Reduction.gov.uk, http://www.crimereduction.gov.uk/fraud10.htm?n23 viewed 12/11/04

Fraud Act 2006, Office of Public Sector Information, http://www.opsi.gov.uk/acts/acts2006/ukpga_20060035_en_1 viewed 23/09/08

Fulcher .J, Scott .J, (1999), *Sociology*, Oxford, Oxford University Press.

Gartenstien-Ross .D, Dabruzzi .K, (2007), *The Convergence of Crime and Terror: Law Enforcement Opportunities and Perils*, Centre for Policing Terrorism, http://www.cpt-mi.org/pdf/The_Convergence_Of_Crime_And_Terrorism.pdf viewed 27/04/09

Giddens .A, (1991), *Modernity and Self Identity*, Cambridge, Polity Press

Grabner .A.S. (2000) *Informal Economy: a report*, HM Treasury

Grayling .C, (2009), *House of Commons Hansard Debates for 06 July 2009*, www.parliment.uk, http://www.publications.parliament.uk/pa/cm200809/cmhansrd/cm090706/debtext/90706-0015.htm viewed 10/08/09

Green Armor Solutions inc, (2007), *Pharming*, Green Armor Solutions inc, http://www.greenarmor.com/pharming.shtml viewed 29/08/08

Grice .A, (March 4 2005), *ID card plan shelved until after election*, Independent, http://www.independent.co.uk/news/uk/politics/id-card-plan-shelved-until-after-election-527163.html viewed 2/08/09

Guardian.co.uk, (2009), *Scrap ID cards plan, says David Blunkett*, http://www.guardian.co.uk/politics/2009/apr/28/blunkett-id-cards#history-byline viewed 14/08/09

Hardin .R, (1998) Trust in Government, in Braithwaite .V, and Levi .M, (eds. 1998) *Trust & Governance*, New York, Russell Sage Foundation

Herring .J, (2006), *Criminal Law: Text, Cases and Materials*, 2nd edition, Oxford, Oxford University Press

Holroyd .P, (2003), Human Traffic, *Intersec*, Vol 3 issue 9

Home Affairs Committee (January 13 2004) *Asylum Applications,* vol 1, The House of Commons
http://www.publications.parliament.uk/pa/cm200304/cmselect/cmhaff/218/218.pdf viewed 16/09/08

Home Affairs Committee, (July 20 2004) *Identity Cards Fourth Report of Session 2003–04 Volume I Report, together with formal minutes,* the House of Commons, London: The Stationery Office

Home Office, (July 2002), *Entitlement Cards and Identity Fraud: A Consultation Paper*, London, The Stationary Office

Home Office, (2005), *Identity Cards: An assessment of awareness and demand for the Identity Cards Scheme*, London, The Stationary Office

Home Office Steering Committee, (2006), *Identity Theft don't become a victim Identity Crime Definitions,* Home Office, http://www.identitytheft.org.uk/definition.html viewed 20/06/07

Home Office Identity Fraud Steering Committee, (February 2 2006) *Updated estimate of the cost of identity fraud to the UK economy*, Home Office, www.identity-theft.org.uk/ID%20fraud%20table.pdf viewed 1/07/07

House of Commons Home Affairs Committee (2003-4) Asylum Applications: Second Report of Session 2003-04 vol 1, London Parliament.uk, http://www.publications.parliament.uk/pa/cm200304/cmselect/cmhaff/218/218.pdf

Howard .J, (2008), *The Captain of Kopenick*, Berlinbilder: Photographs of Berlin, http://berlinbilder.mysite.wanadoo-members.co.uk/koepenick.htm viewed 28/04/08

Huang .F, (2003) *Social Trust, Cooperation, and Human Capital*, Department of Economics, University of Pennsylvania,

Hughes .D, (2000), The Natasha Trade: The Transnational Shadow Market of Trafficking in Women, *Journal of International Affairs*, vol 53 no 2: 625-651 http://www.uri.edu/artsci/wms/hughes/natasha_trade.pdf viewed 5/07/09

ICM, (2009) *U.K. Polling Report*, http://www.icmresearch.co.uk/pdfsearch/search.php?zoom_query=identity+cards&zoom_page=2&zoom_per_page=10&zoom_and=1&zoom_sort=0 viewed 01/08/09

Identity Fraud Steering Committee, (2006) *Updated Estimate of the Cost of Identity Fraud to the UK Economy*, http://www.identitytheft.org.uk/cms/assets/cost_of_identity_fraud_to_the_uk_economy_2006-07.pdf viewed 23/09/08

Identity and Passport Service, (2008a), *What is the National Identity Scheme? How to get your ID card and how it will be produced*, Home Office - Identity and Passport Service Website, http://www.ips.gov.uk/identity/scheme-what-produced.asp#biographical viewed 10/09/08

Identity and Passport Service, (2008b) *Biometric Passports: Is the biometric passport secure?*, Home Office - Identity and Passport Service Website, http://www.ips.gov.uk/passport/about-biometric-secure.asp viewed 10/09/08

Identity and Passport Service, (2008c), *What is the National Identity Scheme? How the scheme will be run,* Home Office - Identity and Passport Service Website, http://www.ips.gov.uk/identity/scheme-what-run.asp#verification viewed 11/09/08

Insall .R, (2000), *Immigrant who sells fake IDs for £4,000*, The People, March 6 page 6

International Association of Chiefs of Police, (March 2002) *Identity Theft: Concepts and Issues Paper*, IACP National Law Enforcement Policy Center, http://www.mrsc.org/ArtDocMisc/Identity%20Theft%20Paper.pdf viewed 12/09/08

Internet World Stats, (2007), *Internet Usage Statistics: The Internet Big Picture*, Internet World Stats, http://www.internetworldstats.com/stats.htm

Jenkins .R, (2004), *Social Identity*,2nd edition, London, Routledge

Jones .G, Levi, M. (2000) 'The value of identity and the need for authenticity', DTI Office of Science and Technology Crime Foresight Panel, http://www.cardiff.ac.uk/socsi/resources/levi-identity.pdf viewed 27/09/08

Johnson .R, Bonsor .K, (March 2006) *How Facial Recognition Systems Work.* How stuff works. http://computer.howstuffworks.com/facial-recognition.htm viewed 7/04/08

Justice, (1995), *Identity Cards Revisited*, London, Institute for Public Policy Research

Judd .T, (March 3 2005), *Internet identity thieves strike once every four minutes*, The Independent, http://www.independent.co.uk/news/uk/crime/internet-identity-thieves-strike-once-every-four-minutes-in-527046.html viewed 25/08/09

Kephart .J, (2005), *Immigration and Terrorism: Moving Beyond the 9/11 Staff Report on Terrorist Travel*, Center for Immigration Studies, www.cis.org

Kyle .D, Liang .Z, (2001), *Migration Merchants: Human Smuggling from Ecuador and China*, Center for Comparative Immigration Studies, Working Paper 43 http://www.no-trafficking.org/content/web/05reading_rooms/China/migration_merchants_human_smuggling_in_china_and_ecuador.pdf viewed 22/06/09

Lague .D, (2006), *Next Step for Counterfeiters: Faking the Whole Company*, The New York Times, http://www.nytimes.com/2006/05/01/technology/01pirate.html?_r=1&scp=1&sq=lague%202006&st=cse viewed 21/04/09

Landesman .M, (2007a) *Phishing scams*, About.com, http://antivirus.about.com/od/emailscams/ss/phishing_3.htm viewed 3/03/08

Landesman .M, (2007b) *Phishing scams*, About.com, http://antivirus.about.com/od/emailscams/ss/phishing_7.htm?p=1 viewed 3/03/08

Legon .N, (2007), *Amnesty for illegal immigrants has been granted*, BBC.co.uk Action Network, http://www.bbc.co.uk/dna/actionnetwork/A11776250 viewed 15/07/07

Levi .M, (2003), 'The Roskill Fraud Commission revisited: An assessment', *Journal of Financial Crime*, vol 11(1), 38-44

Levi .M, Burrows .J, Fleming .M.H, Hopkins .M, Matthews .K, (2007), *The Nature, Extent and Economic Impact of Fraud in the UK*, Report for the Association of Chief Police Officers' Economic Crime Portfolio, http://www.attorneygeneral.gov.uk/attachments/ACPO%20report%20-%20The%20Nature%20Extent%20and%20Economic%20Impact%20of%20Fraud%20in%20the%20UK.pdf viewed 7/06/09

Levi .M, Burrows .J, (2008) Measuring the Impact of Fraud in the U.K. *British Journal of Criminology*, Vol 48, pages 293 - 318

Leyden .J, (2002), *Gummi bears defeat fingerprint sensors*, The Register, http://www.theregister.co.uk/2002/05/16/gummi_bears_defeat_fingerprint_sensors/print.html viewed 16/07/08

Leyden .J, (2005), *Hi-tech no panacea for ID theft woes*, The Register, http://www.theregister.co.uk/2005/09/05/hi-tech_id_theft_cure_fallacy/ viewed 22/09/08

Liberal Democrats, (2009), *Even David Blunkett abandons ID Cards – Huhne*, http://www.libdems.org.uk/documents_detail.aspx?title=Even_David_Blunkett_abandons_ID_Cards_-_Huhne_&pPK=bd4ca257-3656-40e3-8122-04190652d4c3 viewed 14/08/09

Lister .S, (January 18 2005), *How a fake doctor took £1½m and helped 1,000 people to get asylum*, Times Online, http://www.timesonline.co.uk/article/0,,4484-1445773,00.html viewed 14/11/2006

Lormel .D.L, (2002), *Testimony of Dennis M. Lormel, Chief, Terrorist Financial Review Group, FBI Before the Senate Judiciary Committee Subcommittee on Technology, Terrorism and Government Information*, Federal Bureau of Investigation, http://www.fbi.gov/congress/congress02/idtheft.htm viewed 24/ 06/08

Lothene Experimental Archaeology, (2007), *Dr James Barry*, http://www.lothene.demon.co.uk/others/barry.html viewed 05/06/07 page 1 of 1

Luhmann .N, (1988), *Familiarity, Confidence, Trust: Problems and Alternatives*, in Gambetta D, (ed. 1988), Trust: Making and Breaking Cooperative Relations, Oxford, Basil Blackwell

Lyon .D, (November 2004), Identity cards: social sorting by database, *Oxford Internet Institute, Internet Issue Brief no. 3*

MacKinnon .B, (August 9 1997) *Life, the resit*, the Guardian, the Guardian ObserverArchive,
http://guardian.chadwyck.co.uk/guardian/advancedSearchDisplayRecord.do?articleWords=Brian%20MacKinnon&articleWordsContaining=exact&fromDay=01&fromMonth=01&fromYear=1990&toDay=01&toMonth=01&toYear=2000&publication=BOTH&section=&sortType=reverseChronological&pageSize=25&pageNum=1&index=2
Viewed 19/06/07

Malfi .R.D, (2003), *Testimony Before the Committee on Homeland Security: Counterfeit Identification Raises Homeland Security Concerns*, United States General Accounting Office

Malkin .M, (May 24 2006), *Another fake soldier tale debunked,* Real Clear Politics, http://www.realclearpolitics.com/articles/2006/05/another_fake_soldier_tale_debu.html viewed 08/06/07

Mansfield .T, Rejman-Greene .M, (2003), *Feasibility Study on the Use of Biometrics in an Entitlement Scheme*, Centre for Mathematics and Scientific Computing National Physical Laboratory http://dematerialisedid.com/PDFs/feasibility_study031111_v2.pdf viewed 23/05/07

Mead. G.H, (1934), *Mind, self and society from the standpoint of a social behaviourist,* Chicago, The University of Chicago press

Mendham .T, (April 26 2004), *UK Compulsory National Identity Cards (ID Cards) Justifications To Fight Crime and Terror,* Trevor Mendham, http://www.trevor-mendham.com/civil-liberties/identity-cards/fight-crime.html viewed 4/08/2009

Mendham .T, (2004), *UK Compulsory National Identity Cards (ID Cards) To crack down on illegal immigrants,* Trevor Mendham, http://www.trevor-mendham.com/civil-liberties/identity-cards/immigration.html viewed 4/08/2009

Mill J.S, (1863), *Utilitarianism*, London, Parker, Son, and Bourn

Miller .S, (February 27 2003), *Easy to commit, hard to detect: identity scam is growing threat,* The Guardian,
http://guardian.chadwyck.co.uk/noframes/quick/fulltext?ACTION=...
Viewed 25/10/04

Moore .G, (June 12 2007) *The History of Fingerprints*, onin.com,
http://onin.com/fp/fphistory.html viewed 2/07/07

Morris .B, (2004) *Queens speech: The politics of fear*, Independent,
http://www.independent.co.uk/news/uk/politics/queens-speech-the-politics-of-fear-534313.html viewed 3/07/07

National Centre for State Courts (2002), *Individual Biometrics -IRIS SCAN*, National Centre for State Courts,
http://www.bsu.edu/web/ndhoffman/biometrics/biometricsreport.htm viewed 16/09/08

National Consumer Council (N D), *Identity theft: victim support,*
http://www.ncc.org.uk/nccpdf/poldocs/NCC128a_br_ID_theft.pdf viewed 12/09/08

National Criminal Intelligence Service, (2003), *February 2003 Briefing*,
http://www.ncis.co.uk/briefing/270203.asp Viewed 18/03/03

National Health Service- Counter Fraud Service, (April 5 2005), *Egyptian 'Health Tourist' to repay £30,000*, Press Release N.H.S Counter Fraud Service, http://www.cfsms.nhs.uk/doc/press.release/pr.egyptian.health.tourist.04.05.pdf viewed 15/07/07

National Identity Fraud Unit (N D) *Travel Document and Evidence of Identity Information* Department for Works and Pensions

National Missing Person's Helpline, (2005), *Fact file 2005*, www.missingpersons.org viewed 23/09/08

Nielsen .J, (2003), *Usability 101: Introduction to Usability*, Jakob Nielsen's Alertbox, http://www.useit.com/alertbox/20030825.html viewed 7/05/08

Newman .G, Clarke .R, (2003). *Superhighway Robbery: Preventing E-Commerce Crime.* London, Willan Publishing

Newman G.R , McNally M.M, (July 2005) *Identity Theft Literature Review*, National Institute of Justice, Office of Justice Programs, U.S Dept of Justice

Newton .K, (2007), *Social and Political Trust*, in Dalton R.J, Klingemann H.D, (ed. 2007), *Oxford Handbook of Political Behaviour*, Oxford, Oxford University Press

New York Herald, (July 8 1849), *Arrest of the confidence man*, http://chnm.gmu.edu/lostmuseum/lm/328/ viewed 26/06/2006

Nicholas.S, Kershaw.C, Walker.A, (2007), *British Crime Survey 2006/07*, Home Office Statistical Bulletin 11/07, http://www.homeoffice.gov.uk/rds/pdfs07/hosb1107.pdf viewed 6/08/09

Nightscribe.com, (2007), *Wannabes Beware*, http://www.nightscribe.com/Military/SEALs/wannabe_seals.htm viewed 05/06/07

North .R, (2006), *Rachel North*, Justice Not Vengeance, http://www.j-n-v.org/London_Blasts/060712_Rachel_North.htm viewed 1/04/2008

NO2ID, (2009), *Opinion Polls*, NO2ID, http://www.no2id.net/IDSchemes/opinionPolls.php viewed 1/08/09

NO2ID, (2007), *The Problems with 'ID Cards'*, NO2ID, http://www.no2id.net/IDSchemes/whyNot.php viewed 27/07/07

NO2ID, (2008) Identity Cards – Frequently Asked Questions, NO2ID, http://www.no2id.net/IDSchemes/faq.php#3 viewed 3/09/09

Office for Victims of Crime, (2005), *Human Trafficking,* The Office for Victims of Crime, the Office of Justice Programs, U.S. Department of Justice. http://www.ojp.usdoj.gov/ovc/ncvrw/2005/pg5l.html viewed 24/07/09

O'Neil .O, (2002), *A Question of Trust,* Cambridge University Press, Cambridge

O'Neil .S, (2008), *South Africans face visa curb to shut terrorists' route to Britain*, The Times, http://www.timesonline.co.uk/tol/news/politics/article3301166.ece viewed 4/08/09

Online Recruitment - Press Office (2008) *Employees admit to lying at job interview and on their CV to enhance their career prospects,* http://www.onrec.com/content2/printit.asp?id=17826 viewed 30/7/08

Olsen .E.T, (2007), 'Personal Identity', *Stanford Encyclopaedia of Philosophy*, Metaphysics Research Lab, CSLI, Stanford University

Oscherwitz .T, (April 2005), *Synthetic Identity Fraud: Unseen Identity Challenge vol3 No7,* Bank Security News, Royal Media Group Publication, New York, www.royalmedia.com viewed 19/06/07

Parliamentary Office of Science and Technology, (2003), *Government IT projects,* Houses of Parliament, http://www.parliament.uk/post/pr200.pdf viewed 17/08/09

PREM Economic Policy Group and Development Economics Group, (2001), *Assessing Globalization: What is Globalization?* World Bank Group, http://www1.worldbank.org/economicpolicy/globalization/documents/AssessingGlobalizationP1.pdf viewed 08/09/08

Privacy International, (July 22 2002), *ID cards in the UK FAQ,* http://www.privacyinternational.org/article.shtml?cmd(347)=x-347-61875#countries viewed 4/09/08

Privacy International, (October 27 2004), *UK Home Office announces next steps on ID cards,* http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-79530 viewed 4/07/09

Privacy International, (2006), *Leading surveillance societies in the EU and the World 2006,* Privacy International, http://pi.gn.apc.org/article.shtml?cmd[347]=x-347-545269 viewed 7/5/08

Raphaeli .N, (2003), *Ayman Muhammad Rabi' Al-Zawahiri,* Jewish Virtual Library, http://www.jewishvirtuallibrary.org/jsource/biography/Zawahiri.html viewed 27/04/09

Rejman-Greene .M and Mansfield .T, (February 2003), *Feasibility Study on the Use of Biometrics in an Entitlement Scheme*, Middlesex, HMSO http://dematerialisedid.com/PDFs/feasibility_study031111_v2.pdf viewed 3/04/07

Rothstein .B, (2000), Trust, Social Dilemmas and Collective Memories, *Journal of Theoretical Politics*, Vol. 12, No. 4, 477-501
http://www.pol.gu.se/file/Person/Rothstein/TrustRothstein.pdf viewed 24/08/09

Rowlands .A, (2008), *The US and UK are most popular immigration choices*, Emigrate.co.uk, http://www.emigrate.co.uk/news/355342.html viewed 14/05/09

Ruggiero .V, (1996), *Organised and Corporate Crime in Europe*, Aldershot, Dartmouth Publishing

Scott-Joynt .J, (2002), *Losing your identity*, BBC News,
http://news.bbc.co.uk/1/hi/business/2573237.stm viewed 22/05/05

Semmens .N, (2005) 'When the world knows your name: Identity theft and fraud in the UK', *Scottish Journal of Criminal Justice Studies*, Vol. 11, pp. 80-91

Semmens .N, (2006) *'Identity Theft and Fraud'* in Thompson, T. and Black, S. (Eds) Introduction to Biological Human Identification, CRC Press

Serious and Organised Crime Agency, (2007) *SOCA Annual Report 2007-08*, Home Office,
http://www.soca.gov.uk/assessPublications/downloads/SOCA_Annual_Report_0708.pdf viewed 26/08/09

SETimes, (2007), *Another key Serbian war crimes suspect transferred to The Hague*, South Eastern
Times,http://www.setimes.com/cocoon/setimes/print/en_GB/features/setimes/features/2007/06/18/feature-01, viewed 26/06/08

Shukor .S, (December 21 2005), *Postwatch urges tighter controls*, BBC News, http://news.bbc.co.uk/1/hi/england/4549796.stm viewed 21/06/07

Smart .V, (2009), *Adolf Eichmann, His Escape and Capture in Argentina Operation Eichmann,* Holocaust Education & Archive Research Team http://www.holocaustresearchproject.org/trials/eichmanntrialcapture.html viewed 29/07/09

Smilon .M, Hadad .H, Kulstad .M, (2002), *U.S. Announces What Is Believed The Largest Identity Theft Case In American History; Losses Are In The Millions*, U.S Department of Justice, http://www.cybercrime.gov/cummingsIndict.htm viewed 1/09/08

Smith .J.C, (1989), *The Law of Theft, 6th Edition*, London Butterworth's

Smith .P, (2002), Transnational Terrorism and the al-Qaeda Model: Confronting New Realities, *Parameters, US Army War College Quarterly*, pp33-46 http://www.carlisle.army.mil/USAWC/Parameters/02summer/smith.htm viewed 27/04/09

Smith .J, (2008), *The National Identity Scheme – Delivery Plan 2008*, Demos http://www.demos.co.uk/files/File/IDcards_HSspeech.pdf viewed 23/08/09

Smyth .R, (2007) *Twenty years of the forensic conman*, Brief the voice of the Greater Manchester Police, Greater Manchester Police, http://www.gmp.police.uk/mainsite/0/817DE4FA1F265DD8802572D1004931FE/$file/BriefMay2007.pdf viewed 20/08/09

Sniggle.net. (2007), *The Tichborne Claimant*, Sniggle.net, http://www.sniggle.net/tichborne.php viewed 06/06/07

Stana .R.M, (June 25 2002), *Identity Fraud: Prevalence and Links to Alien Illegal Activities*, United States General Accounting Office,

Steinhardt .B, (July 14 2004), *Statement of Barry Steinhardt, Director of the ACLU Technology and Liberty Program, on RFID Tags before the Commerce, Trade and Consumer Protection Subcommittee of the House Committee on Energy and Commerce,* American Civil Liberties Union,
http://www.aclu.org/privacy/spying/15744leg20040714.html viewed 7/07/06

Sugrue .C, (2007) *Ferdinand "Waldo" Demara: The Great Impostor*, CFB Esquimalt Naval & Military Museum,
http://www.navalandmilitarymuseum.org/resource_pages/chars/demara.html viewed 10/09/08

Sullivan .B, (2004) *Your Evil Twin: Behind The Identity Theft Epidemic*, New Jersey, John Wiley & Sons

Summers .C, Toyne .S, (2003), *Gangs preying on cash machines*, BBC News, http://news.bbc.co.uk/go/pr/fr/-/1/hi/uk/3157214.stm viewed 22/06/07

Sydney Morning Herald, (August 29 2005), *Woman exposed as fake doctor is found dead,* Sydney Morning Herald, http://www.smh.com.au/news/world/woman-exposed-as-fake-doctor-is-found-dead/2005/08/28/1125167552522.html Viewed 14/11/2006

Tall .S, (2009), *Huhne: scrap ID cards and put 10,000 bobbies on the beat. Three reasons why he's wrong*, Liberal Democrat Voice, http://www.libdemvoice.org/huhne-scrap-id-cards-and-put-10000-bobbies-on-the-beat-three-reasons-why-hes-wrong-15512.html viewed 14/08/09

Taylor .P, (October 23 2002), *Infiltration of the British Left from the 60s-80s*

Inside Job, The Guardian,
http://www.guardian.co.uk/uk/2002/oct/23/ukcrime.immigrationpolicy viewed 12/08/09

Taylor .P, Funk .C, Clark .A, (2006) *Americans and Social Trust: Who, Where and Why*, Pew Research, http://pewresearch.org viewed 08/5/07

Tempest .M, (January 10 2007), *Reid pledges inquiry into criminal records blunder*, Guardian Unlimited, http://politics.guardian.co.uk/homeaffairs/story/0,,1986954,00.html viewed 15/07/07

Tendler .S, (August 18 2003), *Drug gangs move in on £1.3bn fake documents trade*, The Times,
http://homepage.ntlworld.com/john.masterman/Overkill/Drug%20gangs%20move%20in%20on%20fake%20documents%20trade.pdf viewed 12/07/09

The Stationary Office, (2006) *Identity Cards Bill*, London,

The 419 Coalition, (2009), *Nigeria – The 419 Coalition Website: We fight the Nigerian Scam with Education*, Alpha Electronics Inc., http://home.rica.net/alphae/419coal/

Thomas .D, (December 8 2005), *Tax office shuts credits site after identity theft*, Computing.co.uk http://www.computing.co.uk/computing/news/2147327/tax-office-shuts-credits-site

Turnbull .D, Oliver .J, (December 4 2005), *Victory for MoS as Ministers order probe into DVLA sale of your details*, The Mail on Sunday

Turner .J.C, (1999), *Some Current Issues in Research on Social Identity and Self Categorisation Theories*, in Ellemers N, Spears R, Doosje B, (1999), *Social Identity*, Oxford, Blackwell

Twist .J, (2004), *Testing the Biometric Facts*, BBC News, http://news.bbc.co.uk/1/hi/technology/3659255.stm viewed 12/04/06

U.K. Border Agency, (2009), *Identity cards for foreign nationals*, Home Office, http://www.ukba.homeoffice.gov.uk/managingborders/idcardsforforeignnationals/ viewed 4/08/2009

Ulbricht .K, (2006), *The Captain from Köpenick: The Hundredth Anniversary of a Hoax*, Berlin.de, http://www.berlin.de/ba-treptow-koepenick/derbezirk/koepenickiadeenglisch.html viewed 20/08/09

U.N Development Programme, (2002) *Human Development Report 2002*, http://hdr.undp.org/en/media/HDR_2002_EN_Complete.pdf viewed 23/05/09

Vyavhare .A, (2007) *Breeds of Hackers and Ethical Hacking*, Buzzle.com http://www.buzzle.com/articles/breeds-of-hackers-and-ethical-hacking.html viewed 19/05/09

Walton .J, (2002) *Other countries' ID schemes*, BBC News, http://news.bbc.co.uk/1/hi/uk_politics/2078604.stm viewed 04/09/08

Ward .M, (2003), *Questions over eye scan plan*, BBC News, http://news.bbc.co.uk/go/pr/fr/-/1/hi/technology/3003571.stm viewed 05/11/04

Wigmore .B, (2005), *After 30 years, time runs out on Stopwatch Gang*, Daily Telegraph, http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2005/10/23/wstop23.xml Viewed 10/11/2005

Wignall .A, (March 11 2003 pg 63), *Education: Resources Key Stage 4 Age 14-16: My name's Bond: Derek Bond/*, Guardian, http://guardian.chadwyck.co.uk/noframes/quick/fulltext?ACTION=...

Viewed 25/10/04

Willcox .N.A, and Regan .T.M, (2002), *Identity Fraud: Providing a Solution*, Lexis Nexis,

Woodhouse .C, (March 24 2009), *Scrapping ID cards 'would cost £40m'*, The Independent, http://www.independent.co.uk/news/uk/politics/scrapping-id-cards-would-cost-16340m-1652677.html viewed 17/08/09

Woodward .K, (2000), *Questioning Identity: Gender, Class, Nation*, London, Routledge.

White .R, Haines .F, (1999), *Crime and Criminology – An Introduction*, Oxford, Oxford University Press.

White .M, Hencke .D, Travis .A, (2005), *Government to sacrifice ID card Bill*, The Guardian, http://www.guardian.co.uk/politics/2005/mar/15/uk.houseofcommons1 viewed 14/07/08

Wright .A, (2006), *Organised Crime*, Cullompton, Willan Publishing

Wright .M, (2004), *Mea Culpa*, http://jimtreacher.com/ranger.htm viewed 14/6/07

Ziller .R.C, (1973), *The Social Self*, New York, Pergamon Press

CORRECTION

Appendix 1

The National Fraud Strategic Authority is now the National Fraud Authority

New Estimate of Cost of Identity Fraud to the UK Economy

The table below publishes the new estimate for the cost of identity fraud to the UK Economy - £1.2 billion or around £25 for every adult in Britain.

This new estimate is based on a methodology, developed and agreed by the Identity Fraud Steering Committee members and advised by Home Office economists.

The Identity Fraud Steering Committee (IFSC) was set up by the Home Office in 2003 to work with public and private sector organisations to identify and implement cost effective measures to counter identity fraud. The IFSC comprised the following organisations:

- APACS – the UK payments association;
- Association of Chief Police Officers;
- British Bankers' Association;
- CIFAS, The UK's Fraud Prevention Service;
- Department for Work and Pensions;
- Driver and Vehicle Licensing Agency;
- Finance and Leasing Association;
- Financial Services Authority;
- HM Revenue and Customs;
- Identity and Passport Service;
- Ministry of Justice; and
- Serious Organised Crime Agency.

The IFSC members remain committed to improving awareness, prevention and enforcement to counter identity fraud.

How does this estimate differ from those published earlier?

The first estimate of the cost of identity fraud came from the Cabinet Office report 'Identity Fraud: A Study' in 2002: £1.3 billion.

In February 2006 an updated figure of £1.7 billion, was published, with a breakdown between organisations, following work by the IFSC.

The Government made it clear that the £1.7 billion estimate was a one-off update and future costs exercises would be based on a new more robust methodology that was being devised by the IFSC.

The new methodology devised by the IFSC does not just examine the financial loss to an organisation, but also costs incurred to set systems in place to identify, prevent, deter and prosecute cases of identity fraud.

These are relevant costs as in most cases, these costs would not be incurred if identity fraud was not an issue and it is very likely that if organisations did

not incur these costs, the financial losses to the UK economy would be higher as a result.

The 2002 and 2006 returns were based on the original Cabinet Office methodology and both estimates included the same figures for money laundering, £395m, and VAT 'carousel' fraud, £215m.

These figures have been excluded from the most recent cost estimate exercise as IFSC members feel they do not have a direct link to incidences of identity fraud. In addition figures previously attributed to APACS have included all types of credit card fraud, and for this assessment the APACS figure reflects costs associated with account takeover and application fraud only.

What does this estimate mean?

The updated estimate for the cost of identity fraud has been produced through liaison and discussions with the outlined private and public sector organisations. It represents a best estimate of the scale of the problem at this time which captures available information. Typical of works of this nature, the estimate is likely to be conservative and actual cost may well be higher.

We know from the experience of individuals, the police, and organisations like CIFAS www.cifas.org.uk and APACS www.apacs.org.uk that identity related crime and the overall impact of fraud are a growing concern.

This is the reason that Government has invested £29m in establishing a National Fraud Strategic Authority and Strategy, a Lead Force on Fraud, and a National Fraud Reporting Centre housed within the Lead Force (City of London Police).

The National Fraud Strategic Authority was launched on 1st October 2008.

Estimated Cost of Identity Fraud: 1 April 2006 – 31 March 2007

Organisation / Industry / Sector	Cost of Identity Fraud	Notes
APACS - the UK payments association	£201.2m	Figures include the actual losses associated with Card ID theft, namely account takeover and third party application fraud. It also includes an estimate of the costs associated with the prevention, detection and investigation of identity related crime as specified in the methodology adopted by the Home Office for this exercise. As the banks' fraud prevention and detection systems, the investigation processes and the supporting resource do not solely focus in isolation on identity fraud related crime, these figures can only be regarded as indicative. NOTE: There is potential for overlap with figures reported by CIFAS. APACS and CIFAS have liaised to guard against double counting.
Association of British Insurers	£31m	The cost of internal fraud through re-opening closed claims, dormant accounts and paying claims for personal gain. Also includes account takeover of life policies and cashing joint life policies (estranged spouses).
Audit Commission	£36m	Represents losses from public sector occupational pension schemes due to, for example, next of kin continuing to claim pension payments following the death of a relative.
British Cheque Cashers Association	£0.4m	Estimated direct financial loss and cost of prevention, detection, reporting in relation to cashing of cheques by someone other than the payee.

CIFAS - The UK's Fraud Prevention Service	£23.5m	CIFAS member organisations share information about identified frauds (e.g. application fraud, first party and identity fraud) in the fight to prevent further fraud. Figures relate to costs associated with preventing fraud and actual losses through identity fraud. Typical losses reported by CIFAS members include purchases using credit cards obtained by using false identities and the value of an asset (e.g. a vehicle) purchased from a dealer using finance in a false or stolen identity. NOTE: There is potential for overlap with figures reported by APACS. CIFAS and APACS have liaised to guard against double counting.
Criminal Justice System	£50m	Criminal Justice System costs are an estimate of the total police investigation, prosecution, court and disposal costs for cases of identity fraud.
Driver and Vehicle Licensing Agency	£5.3m	Cost of detecting and investigating applications for driving licences using false identities.
Department for Innovation, Universities and Skills (Student Loans)	£8.4m	Costs relate to setting up systems to investigate fraudulent claims and early estimate of identified losses from student loans obtained using false identities.
Driving Standards Agency	£1.7m	Cost of detecting and investigating identity fraud in the driving test process.
Home Office	£284.4m	Home Office costs relate to the work of its agencies in safeguarding and validating the identities of its customers, as well as costs around deterrence, prevention and investigation of identity fraud.

		The majority of the costs (£227.8m) relate to the operating costs for Identity and Passport Service in carrying out identity checks, investigating suspected identity fraud cases, implementing systems and processes to detect and prevent fraudulent applications of passports, including costs relating to the introduction of face to face interviews for all adult first time applicants for a UK passport. Other costs relate to the work of the Border and Immigration Agency (now UK Border Agency) around operating a dedicated National Document Fraud Unit, deterrence, prevention and investigation of illegal working. Costs have also been included for UK Visas work on prevention of identity fraud.
HM Revenue and Customs	£47.2m	Cost of prevention, detection, investigation and direct financial loss due to ID tax credit fraud.
Ministry of Justice	£35.8m	Cost relates to unpaid fines due to no trace of identity or address. This can be due to a number of reasons such as false or innacurate information being provided and offenders not attending court to verify their details.
Telecommunications UK Fraud Forum	£485m	Estimated cost of obtaining goods and services such as mobile phones, premium rate services, long distance telephone calls through fraudulent applications using false identity details.
Total	**£1,209m**	

----- Original Message -----
From: "James Blindell" <james.blindell@acpr.gov.au>
To: "'T.Holmes'" <sop011@bangor.ac.uk>
Sent: Thursday, March 23, 2006 5:33 AM
Subject: RE: Id fraud Enquiry

> Tim
>
> Current consideration of the ID Card option in Aust. is for crime prevention purposes.
>
> As you say ID crime terms are used interchangeably. One consequence is that it is impossible to get any decent stats. on the extent of losses.
>
> The ACPR, in conjunction with AUSTRAC, has developed some model definitions that will hopefully be signed off by all Australian Police Commissioners in the near future. I set out those proposed definitions below - I stress that, at this stage, they are draft definitions.
>
> Let me know what you think.
>
> Recommendations
>
> 43. It is recommended that:
>
> The term 'identity' encompass the identity of natural persons (living or deceased) and the identity of bodies corporate;
>
> 'Identity Fabrication' be used to describe the creation a fictitious identity;
>
> 'Identity Manipulation' be used to describe the alteration of one's own identity;
10
>
> 'Identity Theft' be used to describe the theft or assumption of a pre-existing identity (or significant part thereof), with or without consent, and, whether, in the case of an individual, the person is living or deceased;
>
> 'Identity Fraud' be used to describe the gaining of money, goods, services other benefits or the avoidance of obligations through the use of a fabricated identity; a manipulated identity; or a stolen/assumed identity;11 and
>
> 'Identity crime' be used as a generic term to describe activities/offences in which a perpetrator uses a fabricated identity; a manipulated identity; or a stolen/assumed identity to facilitate the commission of a crime(s).12
>
> 44. It should be recognised that an 'identity' can be established by a wide range of identifiers including written identifiers (such as drivers licences and passports), biometric identifiers (such as fingerprints and voice prints) and financial identifiers (such as bank account and credit/debit card data);
>

> 45. Given the complexity of the issue (including the issues of intention/fault element, the inclusion of company and other entity names, and the breadth of offences which could be captured by such terms etc.), it may be necessary to undertake further work in this area to more accurately define the various terms used above.
>
> 46. In addition, consideration should be given to obtaining consensus, at least within Australasian law enforcement and revenue protection agencies, in regard to a definition of the underlying concept of 'identity' and of identification related processes such as 'authentication'; 'verification'; 'validation'; and 'registration'.
>
> 10
□□Involves the alteration of one or more elements of identity (e.g. name, date of birth, address) commonly done to dishonestly obtain dual or more access to services or benefits or to avoid established obligations.
>
> 11 Examples of identity fraud include: the use of stolen credit cards or credit card numbers; counterfeiting credit cards; the use of stolen cheques; unauthorised access to online banking services; fraudulently obtaining money, loans, finance and credit; fraudulently obtaining benefits, pensions or entitlements; and evading the payment of taxes, levies or other debts. Identity fraud is a constantly evolving crime type. It is therefore not possible to provide an exhaustive list of the activities that may constitute identity fraud.
>
> 12 Such as: identity fraud and relevant related offences including the possession, distribution and manufacture of relevant items, devices etc.; people smuggling and trafficking; drug trafficking; terrorism
>
>
> Let me know if I can assist further.
>
> Regards
>
> James Blindell
>
> -----Original Message-----
> From: T.Holmes [mailto:sop011@bangor.ac.uk]
> Sent: Wednesday, 22 March 2006 12:44 AM
> To: James Blindell
> Subject: Id fraud Enquiry
>
> Hi
> Thanks for responding the info you have provided is great. I was not
> aware that Australia had considered an identity card scheme.
>
> My study is focused mainly on the idea that id cards can be used to
> prevent crime, specifically id fraud. Have id cards ever been considered

> as a crime prevention tool in Australia?
>
> So far I have found that apart from Australia, the U.S and the U.K no
> one else appears interested in id fraud [even here in the U.K and the
> U.S there is very little research on id fraud].
>
> To make things worse there does not appear to be any consensus on what
> identity fraud is. Some work on id fraud distinguishes between id fraud
> and id theft, others use the term interchangably.
>
> Can you tell me how identity fraud is defined at the ACPR?
>
> Thanks again for the help.
>
> Regards
> Tim Holmes
> --
> T.Holmes sop011@bangor.ac.uk
>
>

Ajaj and Yousef: A Case Study in Fraud

This case study illustrates some of the techniques used by two of the 1993 World Trade Center bombing terrorists to enter and remain in the United States. Almost all of these tactics—italicized here for emphasis—would continue to be used by al Qaeda during the 1990s and in preparation for the 9/11 attack. *Using the services of a travel agent* in Pakistan and traveling under aliases, on August 31, 1992, Ahmad Ajaj and Ramzi Yousef boarded Pakistan International Airlines Flight 703 in Peshawar and flew to Karachi, Pakistan, and then on to Kennedy Airport in New York City. *They sat in first class* during both legs of the trip, believing they would receive less scrutiny there. Between them, they carried a *variety of documents to support their alias identities*, including identification cards, bank records, education records, and medical records.

Upon Ajaj's arrival at Kennedy, the immigration inspector noted that he was traveling on a photo-substituted Swedish passport. Ajaj was sent to secondary immigration inspection,where he claimed he was a member of the Swedish press. His luggage was searched and officers found *a partially altered Saudi passport and a passport from Jordan*, the documents supporting their alias identities, a plane ticket and a British passport in the name of Mohammed Azan, bomb-making manuals, videos and other material on how to assemble weapons and explosives, letters referencing his attendance at terrorist training 48 camps; anti-American and anti-Israeli material, *instructions on document forgery*, and *two rubber stamp devices to alter the seal on passports* issued from Saudi Arabia. The immigration inspector called an agent on the FBI Terrorist Task Force to tell him about

Ajaj, but the agent declined to get involved, instead requesting copies of the file. The inspector also called the Bureau of Alcohol, Tobacco and Firearms, which was "not interested."

Meanwhile, Yousef also was sent to secondary immigration inspection for lacking a passport or a visa that would allow him to enter the United States. He there presented *an Iraqi passport* he allegedly *bought from a Pakistani official for $100*. Upon questioning, Yousef said that the *passport was fraudulent* and that he *bribed a Pakistani official* in order to board the flight. Inspectors also found in his possession an Islamic Center

identity card with Yousef's photo and the name Khurram Khan, under which Ajaj had traveled into the United States. They also found a boarding pass in the name of Mohammed Azan. Although their documents were thus oddly intermingled and both men were in secondary inspection, Yousef was not linked to Ajaj. Rather, Yousef was arrested for not having a visa. He made a *claim for political asylum* and was released into the United States pending a hearing.

Ajaj told authorities he had a political asylum claim from a prior entry in February 1992, and was detained pending a hearing. The evidence suggests that Ajaj left the United States in April 1992, thereby abandoning his asylum claim. In fact, it appears that he *traveled under an alias* to attend a terrorist training camp on the Afghan-Pakistani border.

Ajaj later pleaded guilty to a charge of use of an altered passport and served six months in prison. Not surprisingly, Yousef *never appeared for his hearing*. The World Trade Center was bombed on February 26, 1993. Ajaj was released from prison shortly thereafter, although he had no grounds for remaining in the United States. He was arrested in connection with the attack on March 9, 1993. Yousef was indicted on September 1, 1993, but had left the United States on a *fraudulent Pakistani passport*. He was captured in Pakistan and returned to the United States to stand trial on February 8, 1995.

Although Ajaj was arrested for involvement in the bombing, he did not give up on his political asylum claim. He petitioned for a new attorney and an exclusion hearing—held to determine whether someone is admissible into the United States—in Houston, where he had filed his original political asylum claim. Ajaj's request was denied on April 24, 1993, on the grounds that a passport holder from a visa waiver country who uses a fraudulent passport—Ajaj had used a bogus Swedish passport to enter the United States—is not entitled to such a hearing. Not satisfied with that outcome, Ajaj asked to file *a new political asylum claim* and was given ten days by an immigration judge to do so. Thus, Ajaj was able to file a political asylum claim after his arrest for involvement in the bombing of the World Trade Center.

Yousef was sentenced to 240 years in prison; Ajaj was sentenced to 90 years.

----- Original Message -----
From: "Trevor Mendham" <contact@trevor-mendham.com>
To: <sop011@bangor.ac.uk>
Sent: Thursday, September 07, 2006 8:45 PM
Subject: Re: Identity Cards

> Tim,
>
> You raise some very good questions. I don't have time to respond in
> detail but will make a few points:
>
>> Thank you for responding. I have heard of the National Register but
>> I am unsure
>> as to what threat is posed by this in terms of cvil liberties? [I
>> am aware of
>> the logistical/finnancial nightmare of trying to run this type of
>> system]
>> I have a couple of questions
>> 1}What is it that the national register does that other governement
>> and private
>> databases don't do that makes it such a threat to civil liberties?
>
> It's the arbitrary invasion of privacy. One big, central database
> containing all sorts of information about us. In particular the
> "audit trail" means that the government will have a record of every
> time our card is checked against the central database. This is
> defined in para 9 of Schedule 1:
> http://www.opsi.gov.uk/ACTS/acts2006/60015--b.htm#sch1
> And we can't "opt out".
>
>> 2} Given the way our society works what is the problem with having
>> a national
>> register? We already freely give out masses of information about
>> ourselves to
>> private organisations and government agencies. To play a bit of
>> devils advocate
>> where is the issue of liberty? To be a part of society you have to be
>> recognised by society won't a national register merely formalise
>> what we do
>> every day? If being unknown to the state is a liberty then we all
>> give it up
>> quite early on in life don't we?
>
> You used one vital word: "freely". For example I have chosen NOT to
> use supermarket loyalty cards. I with have no choice about the NIR
> and ID Card.
>
> In addition the existing databases are all "information silos".
> Government departments -and private companies - know what they need
> to know and no more. The NIR turns this principle on it's head and

> says "We'll record everything we can just in case it's useful".
>
> Yes, there are times when we must give up information for society to
> function, I accept that. But currently they are considered necessary
> exceptions rather than the general rule.
>
>> 3} Why is privacy more important than secuirty? Is it better to
>> have privacy
>> and
>> crimes like illegal immigration or is it better to have no privacy
>> but the
>> reassurance that the state knows who every memeber of society is
>> and can verify
>> that information?
>
> There is no evidence that ID Cards will actually stop these crimes
> and give us any significant extra security. Many countries have
> compulsory ID cards and still suffer from illegal immigration, crime
> and terrorism.
>
> Privacy is essential for a free society. Without privacy it's very
> difficult to be different, to be an individual. Or, in political
> terms, a dissident.
>
> That's why privacy is included in article 12 of the Universal
> Declaration of Human Rights:
> http://www.unhchr.ch/udhr/lang/eng.htm
>
> We're supposedly fighting the terrorists in order to preserve our way
> of life. If we give up that way of life then they've won.
>
> - Trevor
>

----- Original Message -----
From: CAMERON, David
To: sop011@bangor.ac.uk
Sent: Friday, February 23, 2007 5:04 PM
Subject: RE: Law & Order

Dear Tim,

Many thanks for taking the time to email regarding Identity Cards.

You may be interested in reading the following article from our website about our campaign to scrap the ID cards scheme;

http://www.conservatives.com/tile.do?def=news.story.page&obj_id=134901

http://www.conservatives.com/tile.do?def=campaigns.display.page&obj_id=134894

I hope this information is useful and good luck with your project.

Yours sincerely,

Anna Biles
Correspondence Secretary
David Cameron's Office
House of Commons
London SW1A 0AA

www.conservatives.com

-----Original Message-----
From: sop011@bangor.ac.uk [mailto:sop011@bangor.ac.uk]
Sent: 16 February 2007 12:51
To: CAMERON, David
Subject: Law & Order

Feedback submitted from the Conservative Party Website.

Name: Tim Holmes
Email: sop011@bangor.ac.uk
Postcode: Postcode not given

Comments:
University Of Wales Bangor Study of Identity Cards and Identity Fraud
Hello my name is Tim Holmes, I am a criminologist from Bangor university. I am studying the use of identity cards as a means of combatting identity fraud. I am trying to include the views and opinions of all the major political parties on the proposed id card scheme in my study and would appreciate any comments or input the Conservative Party could give. My particular interest is in your views on should the id card be introduced and how effective you think it will be in combating crime? Any help you could give my research would be great.

Regards
Tim Holmes

Address: 147.143.83.14
Browser: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB;
rv:1.8.0.9) Gecko/20061206 Firefox/1.5.0.9

----- Original Message -----
From: HANNEY, Matthew
To: sop011@bangor.ac.uk
Sent: Monday, October 30, 2006 6:15 PM
Subject: ID Cards

Tim,

Apologies for not getting back to you sooner.

Below I have outlined the Liberal Democrat position on the points you raised:

1. The government has yet to offer any conclusive proof that ID cards prove beneficial in the prevention of crime. Indeed, it is possible that they would lead to an increase in some crimes, such as fraud. Though the government have insisted that these cards would be impossible to forge, this claim is somewhat implausible. ID cards will become the "holy grail" to fraudsters and terrorists, and with ever developing technology it seems unlikely that we can be definite about their security.

2. There has been no positive link established between the introduction of ID cards and a reduction in crime or terrorism. We are sceptical about the idea that ID cards would reduce illegal immigration. Employers in industries with a high level of illegal immigrant labour are already required to check identity documents before employing someone. It is the blatant disregard to this procedure which needs to be tackled (via inspections), rather than the question of ID cards.

3. Obviously our alternative policies in these wide ranging areas are complex, and I recommend our website (www.libdems.org.uk) for more in-depth information. But our top policies are: with the money saved from not implementing the ID card scheme, we would put 10,000 more police on the street along with investment in extra equipment and new technology.

We do support biometrics passports, believing these would be more effective at tackling cross border fraud, terrorism and illegal immigration. We also propose to establish a National Border Agency, bringing together officers from customs, police and immigration who currently have overlapping responsibilities. We back the use of phone tapping and other 'intercept communications' evidence in court against terrorist suspects.

4. Introducing ID cards in Britain would have a huge social impact. Britain is a country with a strong tradition of civil liberties. Also, unlike every other country with ID cards, the UK does not have a written constitution to protect its citizens. With the relationship between state and citizen not properly defined by law, the risks of an abuse of state power are greater. ID cards will unquestionably tilt the balance of power in the UK away from individuals and towards the government.

The cards could also lead to a culture of mistrust, for example ID cards may be required to keep an appointment with a GP. It may also lead to a growth in discrimination. An increase in racial and ethnic tensions as a result of the introduction of ID card is regrettably an all too likely occurrence.

5. The possible difficulties involved in implementing a scheme on such a large scale are numerous. Yet such errors will have serious implications such as the withholding of benefits and the denial of services.

The government has a woeful history of organising large scale IT projects, with large scale overspending practically the norm. ID cards will be the largest scale public sector IT project undertaken, and considering the failure of smaller government projects such as in the Police Service, Courts Service, CSA and NHS it is not surprisingly that we feel a lack of confidence in the prospects for this scheme.

6. We are sceptical of how reliable any poll finding can be, since the Government still has not come clean about the real cost of this scheme or its draw backs.

I hope that these answers will help. If you have any further questions feel free to get in touch.

Regards,
Matthew

Matthew Hanney
Policy Researcher to Nick Clegg MP
Liberal Democrat Shadow Home Secretary
Tel/Fax: 020 7219 0260

ID Cards Survey

Fieldwork : November 18th-20th 2005

Absolutes/col percents

Table 1

Q.1 The Government has proposed the introduction of identity cards that, in combination with your passport, will cost around £93. From what you have seen or heard do you think that this proposal is a...?

Base: All respondents

			Sex		Age						Social Class				Region				
		Total	Male	Female	18-24	25-34	35-44	45-54	55-64	65+	AB	C1	C2	DE	South East	Mid-lands	North Eng-land	Wales & South West	Scot-land
Unweighted base		1013	455	558	91	166	222	182	168	184	310	215	175	313	269	264	245	143	92
Weighted base		1013	486	527	111	172	203	172	152	203	253	294	213	253	270	264	249	141	89
NET: Good idea		510	233	277	45	98	103	96	71	96	132	144	112	122	131	144	126	60	48
		50%	48%	53%	41%	57%	51%	56%	47%	47%	52%	49%	53%	48%	49%	55%	51%	43%	54%
Very good idea	(4)	141	77	64	5	33	30	21	16	36	47	37	34	24	40	38	32	17	15
		14%	16%	12%	4%	19%	15%	12%	11%	18%	18%	13%	16%	9%	15%	14%	13%	12%	17%
Good idea	(3)	368	156	213	40	66	73	75	55	60	85	107	78	98	91	107	94	43	33
		36%	32%	40%	36%	38%	36%	44%	36%	29%	34%	36%	37%	39%	34%	40%	38%	31%	37%
Bad idea	(2)	246	116	130	33	29	52	36	41	55	56	71	45	74	70	51	56	47	23
		24%	24%	25%	30%	17%	26%	21%	27%	27%	22%	24%	21%	29%	26%	19%	23%	33%	26%
Very bad idea	(1)	235	133	102	33	43	43	37	35	45	62	67	54	52	63	64	62	31	16
		23%	27%	19%	29%	25%	21%	21%	23%	22%	25%	23%	26%	21%	23%	24%	25%	22%	18%
NET: Bad idea		482	249	232	66	71	95	73	76	100	118	138	100	126	132	115	118	77	39
		48%	51%	44%	59%	41%	47%	42%	50%	49%	47%	47%	47%	50%	49%	44%	47%	55%	44%
Don't know/ refused		22	4	18	1	2	4	4	4	6	3	11	1	6	6	5	5	4	2
		2%	1%	3%	1%	1%	2%	2%	3%	3%	1%	4%	1%	2%	2%	2%	2%	3%	2%
Mean		2.42	2.37	2.47	2.16	2.52	2.46	2.47	2.36	2.44	2.46	2.41	2.43	2.38	2.41	2.45	2.39	2.33	2.54
Standard deviation		1.00	1.05	0.95	0.90	1.07	1.00	0.97	0.97	1.04	1.06	0.99	1.04	0.92	1.01	1.02	1.01	0.96	0.98
Standard error		0.03	0.05	0.04	0.10	0.08	0.07	0.07	0.08	0.08	0.06	0.07	0.08	0.05	0.06	0.06	0.06	0.08	0.10

ID Cards Survey

Fieldwork : November 18th-20th 2005

Absolutes/col percents

Table 2
Classification
Base: All respondents

		Total	Sex: Male	Sex: Female	Age: 18-24	Age: 25-34	Age: 35-44	Age: 45-54	Age: 55-64	Age: 65+	Social Class: AB	Social Class: C1	Social Class: C2	Social Class: DE	Region: South East	Region: Mid-lands	Region: North Eng-land	Region: Wales & South West	Region: Scot-land
Unweighted base		1013	455	558	91	166	222	182	168	184	310	215	175	313	269	264	245	143	92
Weighted base		1013	486	527	111	172	203	172	152	203	253	294	213	253	270	264	249	141	89
Sex																			
Male		486	486	-	57	80	91	87	88	84	134	132	115	106	132	126	125	59	45
		48%	100%	-	51%	46%	45%	50%	58%	41%	53%	45%	54%	42%	49%	48%	50%	42%	51%
Female		527	-	527	55	93	111	85	64	119	120	161	98	147	138	138	124	82	44
		52%	-	100%	49%	54%	55%	50%	42%	59%	47%	55%	46%	58%	51%	52%	50%	58%	49%
Age																			
18-24	(21)	111	57	55	111	-	-	-	-	-	21	48	26	16	39	25	31	12	5
		11%	12%	10%	100%	-	-	-	-	-	8%	16%	12%	6%	14%	9%	12%	8%	6%
25-34	(29.5)	172	80	93	-	172	-	-	-	-	57	55	33	27	55	46	36	26	10
		17%	16%	18%	-	100%	-	-	-	-	22%	19%	15%	11%	20%	17%	15%	18%	11%
35-44	(39.5)	203	91	111	-	-	203	-	-	-	66	60	47	30	55	56	52	24	15
		20%	19%	21%	-	-	100%	-	-	-	26%	21%	22%	12%	21%	21%	21%	17%	17%
45-54	(49.5)	172	87	85	-	-	-	172	-	-	43	47	52	30	39	53	35	25	20
		17%	18%	16%	-	-	-	100%	-	-	17%	16%	24%	12%	15%	20%	14%	18%	22%
55-64	(59.5)	152	88	64	-	-	-	-	152	-	35	38	30	48	36	34	39	23	20
		15%	18%	12%	-	-	-	-	100%	-	14%	13%	14%	19%	13%	13%	16%	16%	23%
65+	(70)	203	84	119	-	-	-	-	-	203	32	44	25	101	46	50	56	31	19
		20%	17%	23%	-	-	-	-	-	100%	13%	15%	12%	40%	17%	19%	23%	22%	21%
Average age		46.56	46.36	46.75	21.00	29.50	39.50	49.50	59.50	70.00	43.99	43.40	44.65	54.42	44.09	46.39	47.14	48.04	50.60

ID Cards Survey
Fieldwork : November 18th-20th 2005

Absolutes/col percents

Table 2
Classification
Base: All respondents

		Sex		Age						Social Class				Region				
	Total	Male	Female	18-24	25-34	35-44	45-54	55-64	65+	AB	C1	C2	DE	South East	Mid-lands	North Eng-land	Wales & South West	Scot-land
Weighted base	1013	486	527	111	172	203	172	152	203	253	294	213	253	270	264	249	141	89
Social Class																		
AB	253	134	120	21	57	66	43	35	32	253	-	-	-	76	67	56	29	26
	25%	27%	23%	19%	33%	32%	25%	23%	16%	100%	-	-	-	28%	25%	22%	20%	29%
C1	294	132	161	48	55	60	47	38	44	-	294	-	-	88	64	74	45	23
	29%	27%	31%	43%	32%	30%	27%	25%	22%	-	100%	-	-	33%	24%	30%	32%	25%
C2	213	115	98	26	33	47	52	30	25	-	-	213	-	57	58	53	28	17
	21%	24%	19%	23%	19%	23%	30%	20%	13%	-	-	100%	-	21%	22%	21%	20%	19%
DE	253	106	147	16	27	30	30	48	101	-	-	-	253	49	75	66	39	24
	25%	22%	28%	15%	16%	15%	17%	32%	50%	-	-	-	100%	18%	28%	27%	28%	27%
Region																		
North	338	170	168	36	46	68	54	59	75	82	97	70	90	-	-	249	-	89
	33%	35%	32%	32%	27%	33%	32%	39%	37%	32%	33%	33%	35%	-	-	100%	-	100%
Midlands	316	144	172	28	59	61	63	41	64	74	82	69	90	-	264	-	52	-
	31%	30%	33%	25%	34%	30%	37%	27%	31%	29%	28%	33%	36%	-	100%	-	37%	-
South	359	172	187	48	68	74	55	51	64	97	115	74	73	270	-	-	89	-
	35%	35%	36%	43%	39%	36%	32%	34%	32%	38%	39%	35%	29%	100%	-	-	63%	-

ID Cards Survey
Fieldwork : November 18th-20th 2005

Absolutes/col percents

Table 2
Classification
Base: All respondents

		Sex		Age						Social Class				Region				
	Total	Male	Female	18-24	25-34	35-44	45-54	55-64	65+	AB	C1	C2	DE	South East	Mid-lands	North Eng-land	Wales & South West	Scot-land
Weighted base	1013	486	527	111	172	203	172	152	203	253	294	213	253	270	264	249	141	89
Working status																		
Full-time	450	277	173	46	106	130	109	55	3	146	146	110	47	129	118	101	58	44
	44%	57%	33%	41%	62%	64%	63%	36%	2%	58%	50%	52%	19%	48%	45%	40%	41%	49%
Part-time	113	27	86	11	16	33	21	16	17	30	33	35	16	31	32	31	12	7
	11%	6%	16%	10%	9%	16%	12%	11%	8%	12%	11%	17%	6%	11%	12%	12%	9%	8%
Not working but seeking work or temporarily unemployed/sick	57	29	28	6	16	12	15	7	1	11	12	14	20	16	14	15	7	5
	6%	6%	5%	5%	9%	6%	9%	4%	*	4%	4%	7%	8%	6%	5%	6%	5%	5%
Not working/not seeking work	91	14	77	9	23	21	23	15	-	13	20	22	35	15	24	26	19	7
	9%	3%	15%	8%	13%	11%	13%	10%	-	5%	7%	11%	14%	6%	9%	11%	14%	7%
Retired	247	106	140	1	-	3	3	59	180	42	53	27	123	55	60	65	40	25
	24%	22%	27%	1%	-	1%	2%	39%	89%	17%	18%	13%	49%	20%	23%	26%	29%	29%
Student	53	32	22	38	11	3	1	-	1	11	29	3	10	24	15	9	4	1
	5%	6%	4%	34%	6%	2%	1%	-	1%	4%	10%	1%	4%	9%	6%	4%	3%	1%
Refused	2	1	1	-	1	1	-	-	-	-	1	-	1	-	1	2	-	-
	*	*	*	-	1%	1%	-	-	-	-	*	-	1%	-	*	1%	-	-

ID Cards Survey
Fieldwork : November 18th-20th 2005

Absolutes/col percents

Table 2
Classification
Base: All respondents

		Sex		Age						Social Class				Region				
	Total	Male	Female	18-24	25-34	35-44	45-54	55-64	65+	AB	C1	C2	DE	South East	Mid-lands	North Eng-land	Wales & South West	Scot-land
Weighted base	1013	486	527	111	172	203	172	152	203	253	294	213	253	270	264	249	141	89
Tenure																		
Own outright	324	167	157	18	11	29	43	82	140	78	84	53	109	73	89	87	53	22
	32%	34%	30%	17%	6%	14%	25%	54%	69%	31%	29%	25%	43%	27%	34%	35%	38%	24%
Own with a mortgage	415	193	222	47	86	125	96	40	21	135	136	95	48	106	117	99	58	35
	41%	40%	42%	42%	50%	62%	56%	26%	11%	53%	46%	45%	19%	39%	44%	40%	41%	39%
Council	132	59	73	15	27	22	21	19	28	13	27	30	61	35	28	35	16	17
	13%	12%	14%	13%	16%	11%	12%	13%	14%	5%	9%	14%	24%	13%	11%	14%	11%	19%
Housing Assoc.	35	14	21	4	10	8	3	4	7	5	6	9	16	16	5	5	5	4
	3%	3%	4%	3%	6%	4%	1%	3%	3%	2%	2%	4%	6%	6%	2%	2%	4%	5%
Rented from someone else	88	43	45	23	32	16	7	5	4	20	36	18	14	33	19	17	8	10
	9%	9%	9%	21%	18%	8%	4%	3%	2%	8%	12%	8%	5%	12%	7%	7%	5%	11%
Rent free	6	2	3	2	1	*	1	1	-	*	1	4	1	1	3	1	-	*
	1%	*	1%	2%	1%	*	1%	1%	-	*	*	2%	*	1%	1%	*	-	*
Refused	13	8	5	3	5	2	2	-	2	2	5	3	4	5	2	5	1	*
	1%	2%	1%	3%	3%	1%	1%	-	1%	1%	2%	1%	2%	2%	1%	2%	1%	*

ID Cards Survey

Fieldwork : November 18th-20th 2005

Absolutes/col percents

Table 2
Classification
Base: All respondents

		Sex		Age						Social Class				Region				
	Total	Male	Female	18-24	25-34	35-44	45-54	55-64	65+	AB	C1	C2	DE	South East	Mid-lands	North Eng-land	Wales & South West	Scot-land
Weighted base	1013	486	527	111	172	203	172	152	203	253	294	213	253	270	264	249	141	89
Foreign Holiday in last 3 years																		
Yes	628	304	324	76	115	146	110	75	106	201	198	124	104	182	168	156	75	47
	62%	63%	61%	68%	67%	72%	64%	50%	52%	79%	68%	58%	41%	68%	64%	63%	53%	53%
No	385	182	203	36	57	56	62	77	97	52	95	88	149	88	96	93	66	42
	38%	37%	39%	32%	33%	28%	36%	50%	48%	21%	32%	42%	59%	32%	36%	37%	47%	47%
Number of cars																		
None	205	88	116	19	29	25	28	27	78	24	51	20	110	50	44	60	29	22
	20%	18%	22%	17%	17%	12%	16%	17%	38%	10%	17%	9%	43%	19%	17%	24%	20%	25%
1	441	217	224	40	77	85	66	83	91	100	124	109	107	107	110	116	64	43
	44%	45%	42%	36%	45%	42%	38%	55%	45%	39%	42%	51%	42%	40%	42%	47%	46%	48%
2	286	139	147	38	54	79	57	31	27	101	96	64	25	88	80	57	40	20
	28%	29%	28%	34%	31%	39%	33%	21%	13%	40%	33%	30%	10%	33%	30%	23%	29%	23%
3+	82	42	40	15	13	14	22	11	7	29	23	19	11	24	30	17	8	4
	8%	9%	8%	13%	7%	7%	13%	7%	4%	11%	8%	9%	4%	9%	11%	7%	5%	4%

ID Cards Survey

Fieldwork : November 18th-20th 2005

Absolutes/col percents

Table 2
Classification
Base: All respondents

		Sex		Age						Social Class				Region				
	Total	Male	Female	18-24	25-34	35-44	45-54	55-64	65+	AB	C1	C2	DE	South East	Mid-lands	North Eng-land	Wales & South West	Scot-land
Weighted base	1013	486	527	111	172	203	172	152	203	253	294	213	253	270	264	249	141	89
Internet Access																		
At all	636	317	319	95	126	158	127	78	51	211	208	129	88	189	169	144	81	53
	63%	65%	61%	85%	73%	78%	74%	51%	25%	83%	71%	60%	35%	70%	64%	58%	57%	59%
At home (net)	543	271	272	75	107	140	104	72	44	185	176	114	68	159	150	121	71	43
	54%	56%	52%	68%	62%	69%	60%	48%	22%	73%	60%	54%	27%	59%	57%	48%	50%	48%
At work (net)	285	147	138	27	67	89	64	30	8	130	96	44	15	80	80	66	31	28
	28%	30%	26%	24%	39%	44%	37%	20%	4%	51%	33%	21%	6%	30%	30%	27%	22%	32%
At home	318	153	164	56	54	66	59	47	37	78	100	80	59	96	86	68	46	23
	31%	32%	31%	50%	31%	32%	34%	31%	18%	31%	34%	38%	23%	35%	32%	27%	33%	25%
At work	60	30	31	7	14	15	19	4	1	23	20	10	6	17	15	13	7	9
	6%	6%	6%	6%	8%	7%	11%	3%	*	9%	7%	5%	2%	6%	6%	5%	5%	10%
Both at home and at work	225	118	108	20	53	74	45	26	7	106	75	34	9	63	65	53	24	20
	22%	24%	20%	18%	31%	37%	26%	17%	4%	42%	26%	16%	4%	24%	24%	21%	17%	22%
Somewhere else	32	16	17	13	5	3	4	2	6	3	12	4	13	13	4	10	4	2
	3%	3%	3%	11%	3%	2%	2%	1%	3%	1%	4%	2%	5%	5%	1%	4%	3%	2%
Not at all	377	170	208	16	46	44	45	74	152	42	85	84	166	81	95	105	60	36
	37%	35%	39%	15%	27%	22%	26%	49%	75%	17%	29%	40%	65%	30%	36%	42%	43%	41%

ID Cards Survey
Fieldwork : November 18th-20th 2005

Absolutes/col percents

Table 2
Classification
Base: All respondents

		Sex		Age						Social Class				Region				
	Total	Male	Female	18-24	25-34	35-44	45-54	55-64	65+	AB	C1	C2	DE	South East	Mid-lands	North Eng-land	Wales & South West	Scot-land
Weighted base	1013	486	527	111	172	203	172	152	203	253	294	213	253	270	264	249	141	89
Age Finished Full Time Education																		
Up to 15	208	92	116	5	3	10	34	53	103	24	42	42	100	39	50	59	33	28
	21%	19%	22%	4%	1%	5%	20%	35%	51%	10%	14%	20%	39%	14%	19%	24%	23%	31%
16	263	129	134	19	39	80	53	40	31	49	73	77	65	53	79	72	38	20
	26%	26%	25%	17%	23%	40%	31%	26%	15%	19%	25%	36%	26%	20%	30%	29%	27%	23%
17	81	36	44	11	18	20	13	7	11	15	27	23	16	22	28	15	11	6
	8%	7%	8%	10%	10%	10%	8%	5%	5%	6%	9%	11%	6%	8%	11%	6%	8%	6%
18	126	48	78	28	25	32	20	9	11	40	45	21	20	38	31	34	11	12
	12%	10%	15%	25%	15%	16%	12%	6%	6%	16%	15%	10%	8%	14%	12%	14%	8%	14%
19 or over	256	136	120	18	73	51	44	36	34	110	77	37	32	89	59	56	35	18
	25%	28%	23%	17%	43%	25%	25%	24%	17%	43%	26%	17%	13%	33%	22%	22%	25%	20%
Still in full time education	34	22	12	24	7	1	1	1	-	7	17	3	6	21	6	3	2	2
	3%	5%	2%	22%	4%	*	1%	*	-	3%	6%	2%	3%	8%	2%	1%	2%	3%
Had no full time education	1	-	1	-	1	-	-	-	-	-	-	-	1	-	-	-	1	-
	*	-	*	-	1%	-	-	-	-	-	-	-	*	-	-	-	1%	-
Refused	45	24	20	5	7	7	6	6	13	9	13	9	13	8	12	11	11	3
	4%	5%	4%	5%	4%	4%	4%	4%	6%	4%	5%	4%	5%	3%	5%	4%	8%	3%

ID Cards Survey
Fieldwork : November 18th-20th 2005

Absolutes/col percents

Table 2
Classification
Base: All respondents

		Sex		Age						Social Class				Region				
	Total	Male	Female	18-24	25-34	35-44	45-54	55-64	65+	AB	C1	C2	DE	South East	Mid-lands	North Eng-land	Wales & South West	Scot-land
Weighted base	1013	486	527	111	172	203	172	152	203	253	294	213	253	270	264	249	141	89
Marital Status																		
Single	235	143	92	76	62	38	22	23	14	47	86	45	58	64	67	53	30	20
	23%	29%	17%	68%	36%	19%	13%	15%	7%	18%	29%	21%	23%	24%	26%	21%	21%	22%
Married/ co-habiting	548	258	290	35	97	134	113	80	90	167	141	132	109	157	138	142	70	41
	54%	53%	55%	31%	56%	66%	66%	53%	44%	66%	48%	62%	43%	58%	52%	57%	50%	46%
Widowed/ separated/ divorced	199	70	129	1	10	27	32	42	88	37	58	27	78	45	51	46	32	26
	20%	14%	24%	1%	6%	13%	18%	28%	43%	14%	20%	13%	31%	17%	19%	18%	23%	29%
Refused	31	15	16	-	4	4	6	6	10	3	10	9	9	4	8	8	8	3
	3%	3%	3%	-	2%	2%	4%	4%	5%	1%	3%	4%	3%	1%	3%	3%	6%	3%
Children																		
None aged 18 or under	682	355	327	89	89	67	108	138	190	164	194	127	198	183	172	171	94	62
	67%	73%	62%	80%	52%	33%	63%	91%	94%	65%	66%	60%	78%	68%	65%	69%	67%	70%
NET: Yes	299	115	185	22	79	130	58	7	3	83	91	77	48	83	82	71	39	24
	30%	24%	35%	20%	46%	64%	34%	5%	1%	33%	31%	36%	19%	31%	31%	29%	28%	27%
NET: Yes any aged 15 or under	274	106	168	22	78	121	47	5	2	74	82	72	46	74	76	64	36	23
	27%	22%	32%	20%	45%	60%	27%	3%	1%	29%	28%	34%	18%	27%	29%	26%	26%	26%
- Aged under 5	111	38	72	21	41	40	6	2	-	28	32	27	24	29	32	25	15	10
	11%	8%	14%	19%	24%	20%	3%	1%	-	11%	11%	13%	9%	11%	12%	10%	10%	12%
- Aged 5-10	133	54	79	1	42	65	22	2	2	28	39	43	23	39	36	29	15	13
	13%	11%	15%	1%	25%	32%	13%	1%	1%	11%	13%	20%	9%	15%	14%	12%	11%	15%
- Aged 11-15	122	51	71	1	20	66	34	2	-	38	34	29	21	28	36	31	18	8
	12%	10%	13%	1%	12%	32%	20%	1%	-	15%	12%	14%	8%	10%	14%	13%	13%	9%
- Aged 16-18	72	24	47	-	2	35	29	4	1	26	19	20	7	21	23	19	7	3
	7%	5%	9%	-	1%	17%	17%	3%	*	10%	6%	10%	3%	8%	9%	8%	5%	3%
Refused	32	17	15	-	4	6	6	6	10	6	9	9	8	3	11	7	8	2
	3%	3%	3%	-	2%	3%	3%	4%	5%	2%	3%	4%	3%	1%	4%	3%	6%	3%

ID Cards Survey
Fieldwork : November 18th-20th 2005

Absolutes/col percents

Table 2
Classification
Base: All respondents

		Sex		Age						Social Class				Region				
	Total	Male	Female	18-24	25-34	35-44	45-54	55-64	65+	AB	C1	C2	DE	South East	Mid-lands	North Eng-land	Wales & South West	Scot-land
Weighted base	1013	486	527	111	172	203	172	152	203	253	294	213	253	270	264	249	141	89
Grocery shopping status																		
I am the main grocery shopper in the household	678 67%	237 49%	441 84%	38 34%	121 70%	134 66%	118 69%	115 76%	152 75%	154 61%	193 66%	139 65%	192 76%	166 62%	167 63%	175 70%	105 75%	64 72%
I regularly do the main grocery shop	675 67%	245 50%	429 81%	48 43%	116 67%	138 68%	113 65%	113 74%	147 73%	155 61%	191 65%	143 67%	185 73%	167 62%	171 65%	176 71%	98 69%	63 71%
I regularly do top up grocery shopping (buy items or a basket of itemsas they are needed)	725 72%	301 62%	424 81%	71 64%	132 77%	153 75%	121 70%	106 70%	142 70%	179 71%	214 73%	150 71%	181 72%	196 72%	188 71%	172 69%	102 72%	68 76%
I do not do grocery shopping	145 14%	123 25%	23 4%	34 30%	15 9%	22 11%	30 17%	23 15%	23 11%	46 18%	41 14%	27 13%	32 13%	36 13%	46 17%	38 15%	15 10%	11 12%
Refused	23 2%	14 3%	9 2%	- -	4 2%	5 2%	2 1%	5 3%	7 3%	5 2%	6 2%	7 3%	5 2%	3 1%	8 3%	7 3%	3 2%	1 2%

ID Cards Survey

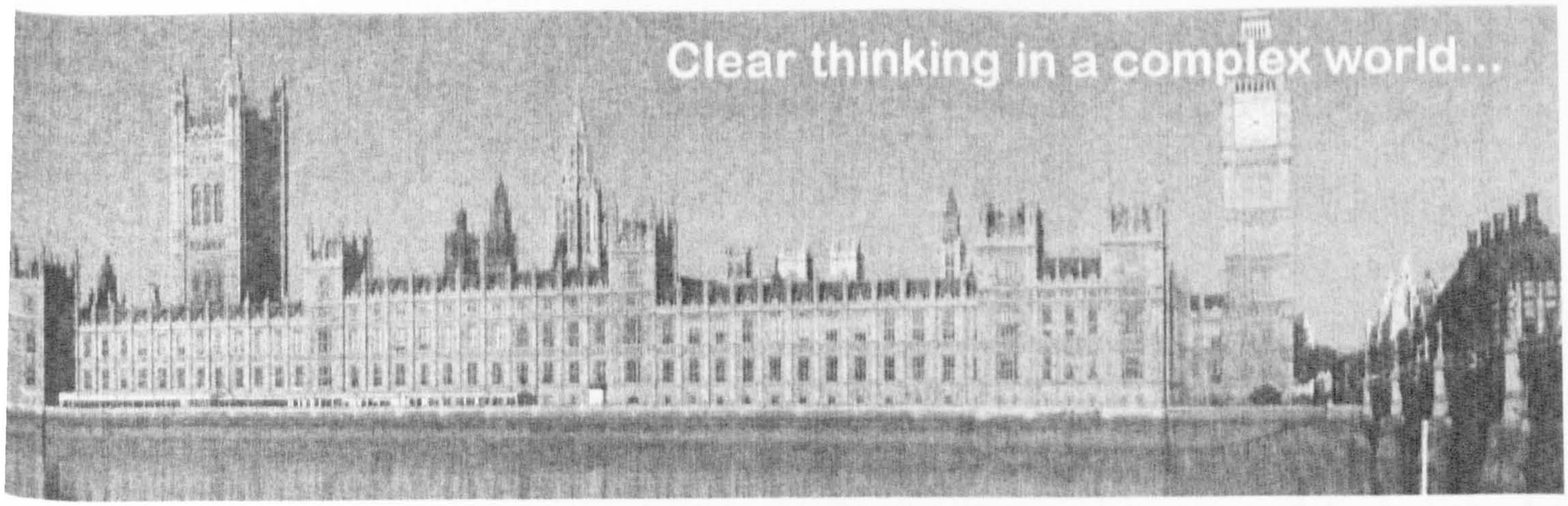
Fieldwork : February 17th-19th 2006

Absolutes/col percents

Table 1

Q.1a The Government has proposed the introduction of identity cards that, in combination with your passport, will cost around £93. From what you have seen or heard do you think that this proposal is a...?
Base: All respondents

			Sex		Age						Social Class				Region				
		Total	Male	Female	18-24	25-34	35-44	45-54	55-64	65+	AB	C1	C2	DE	South East	Mid-lands	North Eng-land	Wales & South West	Scot-land
Unweighted base		1002	449	553	80	150	225	162	188	197	311	230	156	305	267	263	246	139	87
Weighted base		1002	481	521	110	170	200	170	150	200	251	291	210	250	267	261	246	140	88
NET: Good idea		526	229	297	56	95	106	86	78	105	133	140	111	141	136	131	132	83	44
		52%	48%	57%	51%	56%	53%	50%	52%	52%	53%	48%	53%	56%	51%	50%	54%	60%	50%
Very good idea	(4)	162	89	73	14	25	38	29	23	33	46	44	34	38	39	43	41	25	15
		16%	18%	14%	12%	15%	19%	17%	16%	16%	18%	15%	16%	15%	15%	16%	16%	18%	17%
Good idea	(3)	364	141	223	42	70	68	57	54	72	88	96	77	103	97	88	92	58	29
		36%	29%	43%	38%	41%	34%	34%	36%	36%	35%	33%	37%	41%	36%	34%	37%	42%	33%
Bad idea	(2)	259	118	140	27	44	51	44	37	56	60	72	59	68	75	64	70	34	16
		26%	25%	27%	24%	26%	25%	26%	24%	28%	24%	25%	28%	27%	28%	24%	28%	24%	19%
Very bad idea	(1)	197	126	71	25	27	39	39	34	33	52	75	36	34	49	64	39	20	25
		20%	26%	14%	23%	16%	19%	23%	23%	16%	21%	26%	17%	14%	18%	24%	16%	14%	28%
NET: Bad idea		456	244	211	52	72	90	83	71	89	113	147	95	102	124	128	109	54	41
		45%	51%	41%	47%	42%	45%	48%	47%	44%	45%	50%	45%	41%	46%	49%	44%	39%	47%
Don't know		21	7	13	2	3	4	2	2	7	5	4	4	8	7	3	5	2	3
		2%	2%	3%	2%	2%	2%	1%	1%	3%	2%	1%	2%	3%	3%	1%	2%	2%	4%
Mean		2.50	2.41	2.59	2.41	2.56	2.54	2.45	2.45	2.54	2.51	2.38	2.54	2.60	2.48	2.43	2.55	2.64	2.40
Standard deviation		0.99	1.07	0.90	0.98	0.94	1.02	1.03	1.01	0.97	1.03	1.03	0.97	0.91	0.97	1.03	0.96	0.95	1.09
Standard error		0.03	0.05	0.04	0.11	0.08	0.07	0.08	0.07	0.07	0.06	0.07	0.08	0.05	0.06	0.06	0.06	0.08	0.12



ICM Poll for No2ID

Fieldwork dates: 5-6th September 2007

Interview Method: Telephone, unless otherwise stated.

Population effectively sampled: All adults aged 18+

Sampling Method: Within each government office region a random sample of telephone numbers was drawn from the entire BT database of domestic telephone numbers. Each number so selected had its last digit randomised so as to provide a sample including both listed and unlisted numbers.

Sample size: 1,006

Data weighting: Data were weighted to the profile of all adults aged 18+ (including non telephone owning households). Data were weighted by sex, age, social class, household tenure, work status, number of cars in the household and whether or not respondent has taken a foreign holiday in the last 3 years. Targets for the weighted data were derived from the National Readership survey, a random probability survey comprising 34,000 random face-to-face interviews conducted annually.

The data were further weighted by declared votes in the 2005 general election. The weighting scheme is designed as follows:

Questions: The computer tables attached in PDF format show each question, in full, in the order they were put to respondents, all response codes and the weighted and un-weighted bases for all demographics and other data including but not limited that published .

Voting figures: The vote intention cross break in this poll was included for analysis purposes only. ICM's usual vote intention questions were not asked.

Further enquiries: nick.sparrow@icmresearch.co.uk

ID Cards Survey

CATI Fieldwork : September 5th-6th 2007

Absolutes/col percents

Table 1

Q.1 The Government has proposed the introduction of identity cards that, in combination with your passport, will cost around £93. From what you have seen or heard do you think that this proposal is a...?

Base: All respondents

			Gender		Age						Social Class				Region				
		Total	Male	Female	18-24	25-34	35-44	45-54	55-64	65+	AB	C1	C2	DE	South East	Mid-lands	North Eng-land	Wales & South West	Scot-land
Unweighted base		1006	478	528	76	149	188	177	169	247	354	211	174	267	263	252	254	147	90
Weighted base		1006	483	523	119	159	199	169	149	209	262	292	211	241	264	264	248	142	89
NET: Good idea		539	244	295	57	82	113	95	88	104	131	167	121	120	121	151	136	79	51
		54%	50%	56%	48%	51%	57%	56%	59%	50%	50%	57%	57%	50%	46%	57%	55%	56%	58%
Very good idea	(4)	140	74	66	3	18	32	27	27	32	42	49	24	25	30	42	32	20	15
		14%	15%	13%	3%	11%	16%	16%	18%	15%	16%	17%	11%	10%	12%	16%	13%	14%	17%
Good idea	(3)	399	170	229	54	64	82	68	61	72	89	118	97	96	91	109	104	59	36
		40%	35%	44%	45%	40%	41%	40%	41%	34%	34%	40%	46%	40%	34%	41%	42%	42%	41%
Bad idea	(2)	254	114	140	40	47	50	31	29	57	65	70	52	67	86	58	53	35	21
		25%	24%	27%	33%	30%	25%	18%	19%	27%	25%	24%	25%	28%	33%	22%	22%	25%	24%
Very bad idea	(1)	168	113	55	9	21	29	40	27	41	54	42	34	38	44	39	46	25	14
		17%	23%	11%	8%	13%	15%	24%	18%	20%	21%	14%	16%	16%	17%	15%	18%	18%	16%
NET: Bad idea		422	227	195	49	69	80	71	56	98	119	112	85	105	131	97	99	60	35
		42%	47%	37%	41%	43%	40%	42%	37%	47%	46%	38%	40%	44%	50%	37%	40%	42%	40%
Don't know/ refused		45	12	33	13	9	6	3	6	8	11	13	5	16	11	16	13	2	2
		4%	3%	6%	11%	6%	3%	2%	4%	4%	4%	4%	2%	6%	4%	6%	5%	2%	2%
Mean		2.53	2.43	2.62	2.48	2.52	2.60	2.50	2.61	2.47	2.48	2.62	2.54	2.47	2.43	2.62	2.52	2.53	2.60
Standard deviation		0.94	1.02	0.85	0.70	0.88	0.94	1.03	1.00	0.99	1.01	0.94	0.90	0.90	0.92	0.94	0.96	0.95	0.96
Standard error		0.03	0.05	0.04	0.09	0.07	0.07	0.08	0.08	0.06	0.05	0.07	0.07	0.06	0.06	0.06	0.06	0.08	0.10

ID Cards Survey

CATI Fieldwork : September 5th-6th 2007

Absolutes/col percents

Table 2

Q.2 It has been suggested by some police officers that people stopped for traffic violations or littering should have their DNA put on the national DNA database. From what you have seen or heard do you think that this is a...?
Base: All respondents

			Gender		Age						Social Class				Region				
		Total	Male	Female	18-24	25-34	35-44	45-54	55-64	65+	AB	C1	C2	DE	South East	Mid-lands	North Eng-land	Wales & South West	Scot-land
Unweighted base		1006	478	528	76	149	188	177	169	247	354	211	174	267	263	252	254	147	90
Weighted base		1006	483	523	119	159	199	169	149	209	262	292	211	241	264	264	248	142	89
NET: Good idea		483	216	268	48	75	98	69	68	125	111	135	109	129	109	138	141	67	28
		48%	45%	51%	40%	47%	49%	41%	46%	60%	43%	46%	51%	53%	41%	52%	57%	47%	32%
Very good idea	(4)	174	77	97	12	24	41	24	27	46	43	56	27	47	38	39	67	22	9
		17%	16%	18%	10%	15%	20%	14%	18%	22%	16%	19%	13%	20%	14%	15%	27%	15%	10%
Good idea	(3)	310	139	171	36	51	57	45	41	79	69	78	82	81	71	99	74	46	20
		31%	29%	33%	30%	32%	29%	27%	28%	38%	26%	27%	39%	34%	27%	37%	30%	32%	22%
Bad idea	(2)	297	131	167	46	49	62	49	46	45	80	87	67	64	85	71	60	42	39
		30%	27%	32%	39%	31%	31%	29%	31%	21%	31%	30%	32%	26%	32%	27%	24%	30%	44%
Very bad idea	(1)	193	127	66	22	33	35	47	31	27	65	62	30	36	57	49	39	32	17
		19%	26%	13%	19%	21%	17%	27%	21%	13%	25%	21%	14%	15%	22%	18%	16%	22%	19%
NET: Bad idea		491	258	233	69	82	97	95	77	72	145	149	97	99	142	120	99	74	56
		49%	53%	45%	57%	52%	49%	56%	51%	34%	56%	51%	46%	41%	54%	45%	40%	52%	63%
Don't know/ refused		32	10	22	3	2	5	5	5	13	5	8	6	13	13	6	8	1	4
		3%	2%	4%	2%	1%	2%	3%	3%	6%	2%	3%	3%	6%	5%	2%	3%	*	5%
Mean		2.48	2.35	2.59	2.32	2.42	2.53	2.29	2.45	2.73	2.35	2.46	2.51	2.61	2.36	2.50	2.70	2.41	2.24
Standard deviation		1.00	1.04	0.95	0.90	0.99	1.01	1.03	1.03	0.97	1.04	1.04	0.90	0.99	0.99	0.97	1.05	1.00	0.89
Standard error		0.03	0.05	0.04	0.10	0.08	0.07	0.08	0.08	0.06	0.06	0.07	0.07	0.06	0.06	0.06	0.07	0.08	0.10

ID Cards Survey

CATI Fieldwork : September 5th-6th 2007

Absolutes/col percents

Table 3
Classification
Base: All respondents

		Total	Gender		Age						Social Class				Region				
			Male	Female	18-24	25-34	35-44	45-54	55-64	65+	AB	C1	C2	DE	South East	Mid-lands	North Eng-land	Wales & South West	Scot-land
Unweighted base		1006	478	528	76	149	188	177	169	247	354	211	174	267	263	252	254	147	90
Weighted base		1006	483	523	119	159	199	169	149	209	262	292	211	241	264	264	248	142	89
Gender																			
Male		483	483	-	50	70	102	95	71	96	133	138	109	103	137	111	118	73	43
		48%	100%	-	42%	44%	51%	56%	47%	46%	51%	47%	52%	43%	52%	42%	48%	51%	49%
Female		523	-	523	70	89	98	74	79	114	129	153	102	139	126	153	130	69	45
		52%	-	100%	58%	56%	49%	44%	53%	54%	49%	53%	48%	57%	48%	58%	52%	49%	51%
Age																			
18-24	(21)	119	50	70	119	-	-	-	-	-	28	35	26	30	27	30	21	21	20
		12%	10%	13%	100%	-	-	-	-	-	11%	12%	12%	12%	10%	11%	9%	15%	23%
25-34	(29.5)	159	70	89	-	159	-	-	-	-	45	61	33	20	48	32	38	18	23
		16%	15%	17%	-	100%	-	-	-	-	17%	21%	16%	8%	18%	12%	15%	13%	26%
35-44	(39.5)	199	102	98	-	-	199	-	-	-	64	65	49	22	67	51	46	21	13
		20%	21%	19%	-	-	100%	-	-	-	24%	22%	23%	9%	26%	19%	19%	15%	15%
45-54	(49.5)	169	95	74	-	-	-	169	-	-	50	47	35	38	46	45	44	23	11
		17%	20%	14%	-	-	-	100%	-	-	19%	16%	16%	16%	18%	17%	18%	16%	13%
55-64	(59.5)	149	71	79	-	-	-	-	149	-	37	36	31	45	28	47	39	28	8
		15%	15%	15%	-	-	-	-	100%	-	14%	12%	15%	19%	10%	18%	16%	20%	9%
65+	(70)	209	96	114	-	-	-	-	-	209	38	48	37	87	47	59	61	30	13
		21%	20%	22%	-	-	-	-	-	100%	14%	16%	18%	36%	18%	22%	25%	21%	15%
Average age		46.72	47.08	46.39	21.00	29.50	39.50	49.50	59.50	70.00	44.96	44.22	45.59	52.64	45.00	48.27	48.78	47.50	40.22

ID Cards Survey

CATI Fieldwork : September 5th-6th 2007

Absolutes/col percents

Table 3
Classification
Base: All respondents

		Gender		Age						Social Class				Region				
	Total	Male	Female	18-24	25-34	35-44	45-54	55-64	65+	AB	C1	C2	DE	South East	Mid-lands	North Eng-land	Wales & South West	Scot-land
Weighted base	1006	483	523	119	159	199	169	149	209	262	292	211	241	264	264	248	142	89
Social Class																		
AB	262	133	129	28	45	64	50	37	38	262	-	-	-	86	64	63	24	25
	26%	28%	25%	24%	28%	32%	29%	25%	18%	100%	-	-	-	33%	24%	25%	17%	28%
C1	292	138	153	35	61	65	47	36	48	-	292	-	-	64	80	71	47	30
	29%	29%	29%	29%	38%	32%	28%	24%	23%	-	100%	-	-	24%	30%	29%	33%	33%
C2	211	109	102	26	33	49	35	31	37	-	-	211	-	52	50	52	43	15
	21%	23%	20%	22%	21%	24%	21%	21%	18%	-	-	100%	-	20%	19%	21%	30%	16%
DE	241	103	139	30	20	22	38	45	87	-	-	-	241	62	70	62	28	19
	24%	21%	27%	25%	13%	11%	22%	30%	42%	-	-	-	100%	24%	27%	25%	20%	22%
Region																		
North	337	162	175	41	61	59	55	46	74	88	101	67	81	-	-	248	-	89
	33%	34%	33%	35%	38%	30%	33%	31%	35%	34%	35%	32%	34%	-	-	100%	-	100%
Midlands	316	134	182	39	36	57	55	60	69	68	100	69	79	-	264	-	52	-
	31%	28%	35%	33%	22%	28%	33%	40%	33%	26%	34%	33%	33%	-	100%	-	37%	-
South	353	187	166	39	63	83	59	43	66	105	91	75	81	264	-	-	90	-
	35%	39%	32%	33%	39%	42%	35%	29%	31%	40%	31%	36%	34%	100%	-	-	63%	-

ID Cards Survey

CATI Fieldwork : September 5th-6th 2007

Absolutes/col percents

Table 3
Classification
Base: All respondents

		Gender		Age						Social Class				Region				
	Total	Male	Female	18-24	25-34	35-44	45-54	55-64	65+	AB	C1	C2	DE	South East	Mid-lands	North Eng-land	Wales & South West	Scot-land
Weighted base	1006	483	523	119	159	199	169	149	209	262	292	211	241	264	264	248	142	89
Working status																		
Full-time	453	282	171	51	107	131	112	48	4	155	134	112	51	127	94	116	65	50
	45%	58%	33%	43%	67%	66%	66%	32%	2%	59%	46%	53%	21%	48%	36%	47%	46%	56%
Part-time	121	22	99	13	22	38	27	11	10	27	45	26	23	32	40	20	20	9
	12%	5%	19%	11%	14%	19%	16%	7%	5%	10%	15%	12%	9%	12%	15%	8%	14%	10%
Not working but seeking work or temporarily unemployed/sick	54	24	30	10	11	13	12	7	1	3	17	9	25	21	13	13	2	5
	5%	5%	6%	8%	7%	7%	7%	5%	*	1%	6%	4%	11%	8%	5%	5%	2%	5%
Not working/not seeking work	61	10	51	6	15	13	15	11	1	10	11	13	26	15	28	9	4	4
	6%	2%	10%	5%	9%	6%	9%	7%	1%	4%	4%	6%	11%	6%	11%	4%	3%	5%
Retired	269	119	151	-	-	2	4	71	192	50	64	44	112	55	75	83	40	16
	27%	25%	29%	-	-	1%	2%	48%	92%	19%	22%	21%	46%	21%	29%	34%	28%	18%
Student	49	25	23	40	5	2	-	1	-	16	21	7	4	13	14	7	10	5
	5%	5%	4%	34%	3%	1%	-	1%	-	6%	7%	3%	2%	5%	5%	3%	7%	6%

ID Cards Survey
CATI Fieldwork : September 5th-6th 2007

Absolutes/col percents

Table 3
Classification
Base: All respondents

		Gender		Age						Social Class				Region				
	Total	Male	Female	18-24	25-34	35-44	45-54	55-64	65+	AB	C1	C2	DE	South East	Mid-lands	North Eng-land	Wales & South West	Scot-land
Weighted base	1006	483	523	119	159	199	169	149	209	262	292	211	241	264	264	248	142	89
Tenure																		
Own outright	329	160	169	22	10	17	40	89	151	80	92	59	97	64	97	91	44	32
	33%	33%	32%	18%	6%	9%	23%	59%	72%	31%	32%	28%	40%	24%	37%	37%	31%	37%
Own with a mortgage	388	197	191	46	82	131	85	31	13	129	134	82	43	106	100	91	56	36
	39%	41%	37%	39%	52%	66%	50%	21%	6%	49%	46%	39%	18%	40%	38%	37%	40%	40%
Council	130	54	76	31	16	15	25	18	25	15	18	35	61	40	31	29	21	8
	13%	11%	15%	26%	10%	7%	15%	12%	12%	6%	6%	16%	25%	15%	12%	12%	15%	10%
Housing Assoc.	35	15	20	1	9	7	6	3	9	4	11	9	12	15	6	9	2	3
	4%	3%	4%	1%	6%	3%	4%	2%	4%	1%	4%	4%	5%	6%	2%	4%	1%	3%
Rented from someone else	92	45	48	15	35	24	10	6	4	21	31	20	20	31	20	21	13	8
	9%	9%	9%	12%	22%	12%	6%	4%	2%	8%	11%	9%	8%	12%	7%	9%	9%	9%
Rent free	7	4	2	2	2	-	2	*	1	1	2	2	2	3	-	1	3	-
	1%	1%	*	2%	1%	-	1%	*	*	1%	1%	1%	1%	1%	-	*	2%	-
Refused	25	8	17	2	5	6	3	3	6	11	3	4	7	5	9	6	3	1
	2%	2%	3%	2%	3%	3%	2%	2%	3%	4%	1%	2%	3%	2%	4%	3%	2%	1%

ID Cards Survey

CATI Fieldwork : September 5th-6th 2007

Absolutes/col percents

Table 3
Classification
Base: All respondents

		Gender		Age						Social Class				Region				
	Total	Male	Female	18-24	25-34	35-44	45-54	55-64	65+	AB	C1	C2	DE	South East	Mid-lands	North Eng-land	Wales & South West	Scot-land
Weighted base	1006	483	523	119	159	199	169	149	209	262	292	211	241	264	264	248	142	89
Foreign Holiday in last 3 years																		
Yes	604	285	319	74	104	126	101	93	105	200	186	106	112	161	156	155	78	53
	60%	59%	61%	62%	65%	63%	60%	62%	50%	76%	64%	50%	47%	61%	59%	62%	55%	60%
No	402	198	205	45	55	73	68	56	104	62	106	105	129	102	107	93	64	35
	40%	41%	39%	38%	35%	37%	40%	38%	50%	24%	36%	50%	53%	39%	41%	38%	45%	40%
Number of cars																		
None	209	86	123	23	34	13	36	30	73	30	48	27	103	72	47	45	22	23
	21%	18%	24%	20%	22%	6%	22%	20%	35%	12%	17%	13%	43%	27%	18%	18%	16%	26%
1	418	203	216	32	70	100	58	64	95	109	131	83	96	112	101	114	63	29
	42%	42%	41%	27%	44%	50%	34%	43%	45%	42%	45%	39%	40%	42%	38%	46%	44%	32%
2	289	151	138	36	40	71	58	43	40	95	81	80	32	61	92	69	41	27
	29%	31%	26%	30%	25%	36%	34%	29%	19%	37%	28%	38%	13%	23%	35%	28%	29%	30%
3+	90	43	47	28	15	15	17	13	2	27	31	22	10	19	24	21	16	10
	9%	9%	9%	23%	9%	7%	10%	9%	1%	10%	11%	10%	4%	7%	9%	8%	11%	12%

ID Cards Survey

CATI Fieldwork : September 5th-6th 2007

Absolutes/col percents

Table 3
Classification
Base: All respondents

		Gender		Age						Social Class				Region				
	Total	Male	Female	18-24	25-34	35-44	45-54	55-64	65+	AB	C1	C2	DE	South East	Mid-lands	North Eng-land	Wales & South West	Scot-land
Weighted base	1006	483	523	119	159	199	169	149	209	262	292	211	241	264	264	248	142	89
Internet Access																		
At all	771 77%	390 81%	381 73%	111 93%	141 89%	186 93%	144 85%	104 70%	85 41%	235 90%	250 86%	161 76%	126 52%	199 76%	206 78%	188 76%	109 77%	69 77%
At home (net)	682 68%	349 72%	333 64%	97 81%	123 77%	168 84%	123 73%	94 63%	77 37%	217 83%	210 72%	146 69%	108 45%	170 64%	184 70%	166 67%	97 68%	66 74%
At work (net)	362 36%	189 39%	172 33%	55 46%	92 58%	95 48%	82 49%	30 20%	6 3%	153 59%	132 45%	46 22%	30 12%	110 42%	81 31%	89 36%	44 31%	39 44%
At home	381 38%	188 39%	193 37%	49 41%	47 29%	85 43%	57 34%	70 47%	73 35%	78 30%	111 38%	108 51%	84 35%	82 31%	118 45%	88 36%	64 45%	29 33%
At work	61 6%	28 6%	32 6%	7 6%	16 10%	13 6%	16 9%	7 5%	2 1%	14 5%	33 11%	9 4%	5 2%	22 8%	15 6%	11 4%	11 8%	2 2%
Both at home and at work	301 30%	161 33%	140 27%	48 40%	76 48%	83 42%	67 39%	24 16%	4 2%	140 53%	99 34%	38 18%	25 10%	88 33%	66 25%	78 31%	33 23%	36 41%
Somewhere else	29 3%	13 3%	16 3%	7 5%	3 2%	5 3%	4 3%	3 2%	6 3%	4 2%	6 2%	6 3%	12 5%	8 3%	7 3%	11 4%	2 1%	1 1%
Not at all	234 23%	92 19%	142 27%	9 7%	18 11%	13 7%	26 15%	45 30%	123 59%	27 10%	42 14%	50 23%	116 48%	64 24%	58 22%	59 24%	33 23%	20 23%
Refused	1 *	1 *	- -	- -	- -	- -	- -	- -	1 *	- -	- -	1 *	- -	- -	- -	1 *	- -	- -

ID Cards Survey
CATI Fieldwork : September 5th-6th 2007

Absolutes/col percents

Table 3
Classification
Base: All respondents

		Gender		Age						Social Class				Region				
	Total	Male	Female	18-24	25-34	35-44	45-54	55-64	65+	AB	C1	C2	DE	South East	Mid-lands	North Eng-land	Wales & South West	Scot-land
Weighted base	1006	483	523	119	159	199	169	149	209	262	292	211	241	264	264	248	142	89
What is the highest educational level that you have achieved to date?																		
Secondary/ high school/ NVQ 1-3	558	256	302	78	71	109	90	92	119	95	144	157	162	148	147	141	79	44
	55%	53%	58%	65%	44%	55%	53%	61%	57%	36%	49%	74%	67%	56%	56%	57%	56%	49%
University degree or equivalent professional qualification/ NVQ4	273	137	136	28	65	58	48	39	35	107	104	22	40	70	67	72	32	32
	27%	28%	26%	23%	41%	29%	28%	26%	17%	41%	36%	10%	16%	27%	25%	29%	23%	36%
Higher university degree/ Doctorate/ MBA/ NVQ 5 or equivalent	74	43	32	10	15	15	15	7	12	44	19	3	7	23	20	15	6	9
	7%	9%	6%	8%	10%	8%	9%	5%	6%	17%	7%	2%	3%	9%	8%	6%	5%	11%
None of these	74	38	36	4	3	12	13	7	34	8	18	22	26	17	20	15	19	2
	7%	8%	7%	4%	2%	6%	8%	5%	16%	3%	6%	10%	11%	6%	8%	6%	14%	2%
Refused	27	9	17	-	5	5	3	4	9	7	6	7	7	6	10	5	4	2
	3%	2%	3%	-	3%	3%	1%	3%	4%	2%	2%	3%	3%	2%	4%	2%	3%	2%

ID Cards Survey

CATI Fieldwork : September 5th-6th 2007

Absolutes/col percents

Table 3
Classification
Base: All respondents

		Gender		Age						Social Class				Region				
	Total	Male	Female	18-24	25-34	35-44	45-54	55-64	65+	AB	C1	C2	DE	South East	Mid-lands	North Eng-land	Wales & South West	Scot-land
Weighted base	1006	483	523	119	159	199	169	149	209	262	292	211	241	264	264	248	142	89
Marital Status																		
Single	225 22%	122 25%	103 20%	90 75%	45 28%	28 14%	28 16%	16 10%	18 9%	57 22%	80 27%	35 17%	53 22%	71 27%	36 14%	56 23%	29 21%	33 37%
Married/ co-habiting	584 58%	302 63%	282 54%	30 25%	99 62%	147 74%	104 61%	97 65%	108 52%	171 65%	166 57%	145 68%	102 42%	142 54%	169 64%	145 58%	84 59%	44 50%
Widowed/ separated/ divorced	181 18%	54 11%	126 24%	- -	11 7%	20 10%	36 21%	36 24%	78 37%	29 11%	43 15%	27 13%	81 34%	48 18%	52 20%	44 18%	26 19%	10 12%
Refused	16 2%	4 1%	12 2%	- -	4 3%	4 2%	3 1%	1 1%	4 2%	5 2%	2 1%	4 2%	5 2%	3 1%	7 3%	3 1%	2 2%	1 1%
Children																		
None aged 18 or under	694 69%	349 72%	345 66%	102 85%	78 49%	65 33%	103 61%	141 94%	205 98%	171 65%	204 70%	134 63%	186 77%	184 70%	171 65%	181 73%	103 73%	54 61%
NET: Yes	292 29%	128 27%	164 31%	18 15%	77 48%	128 64%	62 37%	7 5%	1 *	84 32%	85 29%	73 35%	50 21%	75 29%	86 32%	63 26%	35 25%	33 37%
NET: Yes any aged 15 or under	269 27%	116 24%	154 29%	18 15%	74 46%	124 62%	48 28%	5 3%	1 *	78 30%	79 27%	67 31%	46 19%	73 28%	78 30%	60 24%	28 20%	31 34%
- Aged under 5	105 10%	38 8%	67 13%	16 13%	54 34%	30 15%	5 3%	- -	- -	21 8%	30 10%	34 16%	20 8%	22 8%	36 13%	22 9%	13 9%	13 14%
- Aged 5-10	134 13%	57 12%	78 15%	6 5%	33 21%	75 37%	18 11%	2 1%	1 *	50 19%	34 12%	29 14%	21 9%	40 15%	37 14%	30 12%	11 8%	16 18%
- Aged 11-15	127 13%	61 13%	66 13%	3 3%	12 8%	71 35%	36 21%	4 3%	- -	35 13%	39 13%	31 15%	22 9%	35 13%	39 15%	27 11%	13 9%	13 15%
- Aged 16-18	64 6%	34 7%	30 6%	3 3%	3 2%	23 12%	31 19%	3 2%	- -	16 6%	15 5%	20 10%	13 5%	17 7%	22 8%	10 4%	11 7%	4 4%
Refused	20 2%	6 1%	13 3%	- -	4 3%	6 3%	4 2%	2 1%	4 2%	7 3%	3 1%	4 2%	5 2%	4 2%	7 3%	4 2%	3 2%	2 2%

----- Original Message -----
From: "T.Holmes" <sop011@bangor.ac.uk>
To: <bgivens@privacyrights.org>
Sent: Monday, March 20, 2006 3:05 PM
Subject: U.K. Id fraud study

> Hello
> My name is Tim Holmes I am a researcher at the University of Wales
> Bangor. I am conducting a study in to id fraud in the U.K and the
> possible impact of an id card system on this type of crime.
>
> I was hoping you could help me, as part of my study I am looking in to
> identity fraud in America, in particular when did identity
> fraud/identity theft become a big issue in America, and how has your
> country responded.
>
> Any help you could give my study would be greatly appreciated.
>
> Regards
> Tim Holmes
> --
> T.Holmes sop011@bangor.ac.uk
>
>

----- Original Message -----
From: "Beth Givens" <bgivens@privacyrights.org>
To: "T.Holmes" <sop011@bangor.ac.uk>
Sent: Saturday, March 25, 2006 9:30 PM
Subject: Re: U.K. Id fraud study

> Hello and sorry for the delay in responding.
>
> I wish I had the answers to your questions in a single document -- or
> I could point you to a history of id theft in the U.S. Unfortunately,
> I don't have such a document at my fingertips. And to give you my
> assessment would take more time than I have, sorry to say. It's a big topic.
>
> The first hearing on the topic was held by the Federal Trade
> Commission in 1996. You might be able to find some useful info in the
> materials associated with that hearing (they call their hearings
> workshops). I believe you'll find the transcripts here:
> http://www.ftc.gov/bcp/workshops/idtheft/index.html
>
> Here are some links that you might find useful for older materials:
> http://www.ftc.gov/os/1998/05/identhef.htm
> http://www.ftc.gov/os/1998/05/identhef.htm
>
> ANd we have a page that links you to various id theft surveys:
> http://www.privacyrights.org/ar/idtheftsurveys.htm
>
> Good luck!
>
> Beth Givens
>
> At 06:05 AM 3/20/2006, you wrote:
>>Hello
>>My name is Tim Holmes I am a researcher at the University of Wales
>>Bangor. I am conducting a study in to id fraud in the U.K and the
>>possible impact of an id card system on this type of crime.
>>
>>I was hoping you could help me, as part of my study I am looking in
>>to identity fraud in America, in particular when did identity
>>fraud/identity theft become a big issue in America, and how has your
>>country responded.
>>
>>Any help you could give my study would be greatly appreciated.
>>
>>Regards
>>Tim Holmes
>>--
>>T.Holmes sop011@bangor.ac.uk
>
> The information, advice, and suggestions contained in this email
> should be used as an information source and not as legal advice.

>
> Beth Givens, Director
> Privacy Rights Clearinghouse
> 3100 - 5th Ave., Suite B
> San Diego, CA 92103
> Voice: 619-298-3396
> Fax: 619-298-5681
> bgivens@privacyrights.org
> http://www.privacyrights.org
> ++
> Join our email newsletter.
> http://www.privacyrights.org/subscribe.html
>
>

----- Original Message -----
From: "T.Holmes" <sop011@bangor.ac.uk>
To: "Beth Givens" <bgivens@privacyrights.org>
Sent: Monday, March 27, 2006 1:04 PM
Subject: U.K. Id fraud study

> Hi
> Thanks for responding to my e-mail. I am about to look through the stuff
> you have sent me. I would have liked a big history of id theft in the
> U.S but I am not surprised that it isn't easy to find. From my research
> I have found that id theft/id fraud is a subject which generally doesn't
> receive much academic attention or research. [Apart from the U.S and the
> U.K the only other place in the world that looks at Id fraud is Australia]
>
> Thanks for the information
>
> All the Best
> Tim Holmes
> --
> T.Holmes sop011@bangor.ac.uk
>
>

----- Original Message -----
From: "Beth Givens" <bgivens@privacyrights.org>
To: "T.Holmes" <sop011@bangor.ac.uk>
Sent: Monday, March 27, 2006 8:55 PM
Subject: Re: U.K. Id fraud study

>I know of a PhD student who is studying id theft for her
> dissertation. She's from Rutgers Univ and is visiting my office later
> this week.
>
> Her contact info is:
> Megan McNally
> mmm151@pegasus.rutgers.edu
>
> Perhaps she has run across a general history of the subject.
>
> Another possible resource is Judith Collins, PhD, of Michigan State
> Univ. She has established an id theft center
> judithc@msu.edu
> www.cj.msu.edu/~outreach/identity/
>
> Good luck!
>
> bg
>
> At 04:04 AM 3/27/2006, you wrote:
>>Hi
>>Thanks for responding to my e-mail. I am about to look through the
>>stuff you have sent me. I would have liked a big history of id theft
>>in the U.S but I am not surprised that it isn't easy to find. From
>>my research I have found that id theft/id fraud is a subject which
>>generally doesn't receive much academic attention or research.
>>[Apart from the U.S and the U.K the only other place in the world
>>that looks at Id fraud is Australia]
>>
>>Thanks for the information
>>
>>All the Best
>>Tim Holmes
>>--
>>T.Holmes sop011@bangor.ac.uk
>
> The information, advice, and suggestions contained in this email
> should be used as an information source and not as legal advice.
>
> Beth Givens, Director
> Privacy Rights Clearinghouse
> 3100 - 5th Ave., Suite B
> San Diego, CA 92103
> Voice: 619-298-3396

> Fax: 619-298-5681
> bgivens@privacyrights.org
> http://www.privacyrights.org
> ++
> Join our email newsletter.
> http://www.privacyrights.org/subscribe.html
>
>

----- Original Message -----
From: <mmm151@pegasus.rutgers.edu>
To: "T.Holmes" <sop011@bangor.ac.uk>
Sent: Wednesday, March 29, 2006 4:21 PM
Subject: Re: U.K ID FRAUD Study

> Hi Tim,
> I'm still in the process of trying to answer some of these questions
> myself, but I'll be happy to share what I do know. You may already have
> this (see attached), but you might want to take a look at the literature
> review I co-wrote, which generally covers the state of identity theft in
> the U.S. through the end of 2004. The basic conclusion is that the issue
> over here is a big mess and it has actually gotten worse in the past year.
>
> The terms "identity theft" and "identity fraud" are often used
> interchangeably here - and its been almost 10 years since it was first
> criminalized. There really is no consensus on their relationship, but my
> basic understanding is that identity fraud describes an instance in which
> someone fraudulently claims to be another person (whether real or
> ficticious). In this way, identity theft is a subcategory of identity
> fraud (some also consider both to be categories of "identity crime").
> Identity fraud is also defined in relation to "third parties" - that is an
> institution of some type, while identity theft can only properly be used
> in relation to the owner of an identity. Generally, this means an
> individual, but some collective identities have been "stolen" (i.e.,
> fraudulent activities are committed using the name of an institution).
>
> I'm not that familiar with the UK literature, but here the term is also
> used to describe credit card and bank fraud, which frankly is rediculous.
>
>> Hello
>> My name is Tim Holmes I am a Phd student at the University of Wales
> Bangor. I am conducting a study assessing the impact of an identity card
> system [which the U.K will adopt in 2008] on the levels and nature of
> identity fraud in the U.K.
>>
>> As part of my study I am looking at id theft U.S.A, I was told that you
> are also studying identity theft and may be able to help me. I am trying
> to establish the development of id theft in your country- when was the
> term first used and why.
>>
>> I am also trying to establish what definitions of id theft/ id fraud are
> used in the U.S. Here in the U.K [and in Australia] there is no
>> consensus on what constitutes id theft and whether or not it is
>> different to id fraud.
>>
>> Any help you could give me would be greatly appreciated.
>>
>> Regards
>> Tim Holmes

>> --
>> T.Holmes sop011@bangor.ac.uk
>>
>>
>
>

----- Original Message -----
From: <mmm151@pegasus.rutgers.edu>
To: "T.Holmes" <sop011@bangor.ac.uk>
Sent: Wednesday, March 29, 2006 5:47 PM
Subject: Re: U.K ID FRAUD Study

> Hi Tim,
> Sorry, but I think I accidentally sent you half an email earlier. I'm not
> sure what got sent so some of this may be repeated.
>
> I'm still in the process of trying to answer some of these questions
> myself, but I'll be happy to share what I do know. You may already have
> this (see attached), but you might want to take a look at the literature
> review I co-wrote, which generally covers the state of identity theft in
> the U.S. through the end of 2004. The basic conclusion is that the issue
> over here is a big mess and it has actually gotten worse in the past year.
> I am working to update this review as part of my dissertation, but I
> won't be finished until this summer.
>
> The terms "identity theft" and "identity fraud" are often used
> interchangeably here - and its been almost 10 years since it was first
> criminalized. There really is no consensus on their relationship, but my
> basic understanding is that identity fraud describes an instance in which
> someone fraudulently claims to be another person (whether real or
> ficticious). In this way, identity theft is a subcategory of identity
> fraud (some also consider both to be categories of "identity crime").
> Identity fraud is also defined in relation to "third parties" - that is an
> institution/business of some type, while identity theft can only properly
> be used in relation to the owner of an identity. Generally, this means an
> individual, but some collective identities have been "stolen" (i.e.,
> fraudulent activities are committed using the name of an institution). As
> such, when an offender uses my name to open a new credit card account, I
> am a victim of identity theft (because it's my identity) while the credit
> card company and any business in which the account is used are victims of
> identity fraud.
>
> I'm not that familiar with the UK literature, but here the term is also
> used to describe credit card and other types of routine fraud, which
> frankly is rediculous. The term "true name fraud" was developed by the
> credit card industry (and perhaps used in some other types of financial
> industries) to distinguish real identities (individuals) from fake
> identities. Now the term is used (albeit sparingly) to describe what I

> consider to be the real victims of identity theft - those whose identities
> are actually assumed. Generally, this can be understood as "new
> activities" or when an offender uses a victim's name/personal information
> to lead a sort of parallel life. They may open a new line of credit,
> obtain a loan or employment, or give the information to the police.
> Essentially, the victim can be unaware of new activities for a long time -
> at least as long as it takes for the offender's actions to catch up to
> them. But as I mentioned, the term is also used to describe a number of
> "existing activities" - when offenders misuse existing resources (bank,
> credit card, Internet/email, telephone and utilities accounts). So, in
> other words, the victims life/lifestyle is directly affected but they find
> out about it sooner and they are unlikely to suffer damages as a result.
>
> To complicate these matters even more, the term identity theft is now used
> to describe any instance in which personal information is wrongfully
> obtained, particularly in relation to database breaches. In my opinion,
> the offense of identity theft has not been completed until the information
> has been misused, but the potential for such misuse is largely being
> exploited in the absence of evidence that anything happened as a result of
> a breach.
>
> In terms of where the term came from, the first U.S. reference to
> "identity theft" I have found is in a 1989 article published in the
> Sun-Sentinel (Florida), entitled " Identity theft besmirches victims'
> records." (I have not specifically searched the literature of other
> countries for the origin of the term, so if you have any information about
> this I'd appreciate it). I've actually been in touch with the author
> (Mike Billington) who claims his editor really came up with the term. I
> haven't been able to track down the editor to find out whether he heard
> the term from someplace else, but I do doubt that he actually conied the
> term. The first reference to the term "identity thief" actually appeared
> seven years earlier in the 1982 obituary of Ferdinand Waldo Demara, Jr.
> His life story was the inspiration for the 1959 book/1960 movie "The Great
> Imposter." I just got my hands on the book, and I'm trying to find out
> whether the term identity theft was specifically used. At any rate, it is
> a common sense way to describe it, so who knows where it actually came
> from. Before that, there were a number of cases of "identity assumption"
> or "assumed identity", which obviously refers to the same thing. I've got
> newspaper stories going back to the 1800's that fit the description of
> what is now collectively known as identity theft, and there are a handful
> of historical examples practically dating back to the bible...not to
> mention literary examples like the Prince and the Pauper.
>
> The question of why the term is used now is more difficult to answer - and
> its actually one of the questions I'm trying to answer in my research.
> The party line is that its a product of the information age (specifically
> the use of computers and the Internet, and our increasing reliance on
> information to conduct routine business). This makes a certain amount of
> sense, but its really speculation. There's no specific evidence to back
> this up right now, particularly with regard to the use of computers or the

> Internet either to obtain personal information or misuse it. The second
> half of the party line is that it was criminalized to recognize individual
> victims (i.e., the shift from identity fraud to theft). Before the
> mid-1990s, individuals were not considered victims of "identity fraud".
> There is something fishy about this to me though since
> the laws that criminalized identity theft really have nothing to do with
> victims.
>
> I'm actually leaving for California on Friday to speak with some of the
> people who were involved with the initial movement to criminalize identity
> theft. The whole thing seems to have generated from public interest
> groups there, so I'm going to find out for myself what actually happened
> since there is little published before 1998. I also have some interviews
> scheduled for when I return with a few other people who were involved in
> the beginning. Hopefully, I'll have a better answer to this in a few
> weeks and I'll let you know what I find out.
>
> As for my personal opinion, I believe identity assumption is a problem
> because it can seriously damage individual lives and is a real pain to
> clear up, but these cases only constitute about one-third (or 1.5% of the
> population) of the 10 million victims estimated by our government. The
> rates are inflated because they've included credit card fraud, but
> underestimated to a degree because they exclude deceased victims and
> children under the age of 18. My research, therefore, is examining the
> use of identity theft as a pretext for other agendas. Specifically, I'm
> looking at the phenomenon as a moral panic, and I believe the whole thing
> is tied to the aftermath of 9/11. From what I've found so far, there was
> actually very little attention paid to the topic before 2002 even when the
> entire country was rushing to criminalize it, but its now a household term
> that is used without qualification.
>
> I hope all of this helps. As you might have guessed, I could talk about
> this stuff for hours. I'm also interested in hearing your perspectives on
> the development of identity theft in the UK. I will be gone for about a
> week, but I will let you know what I come up with after the interviews are
> complete.
>
> Megan
>
>
>> Hello
>> My name is Tim Holmes I am a Phd student at the University of Wales
> Bangor. I am conducting a study assessing the impact of an identity card
> system [which the U.K will adopt in 2008] on the levels and nature of
> identity fraud in the U.K.
>>
>> As part of my study I am looking at id theft U.S.A, I was told that you
> are also studying identity theft and may be able to help me. I am trying
> to establish the development of id theft in your country- when was the
> term first used and why.

>>
>> I am also trying to establish what definitions of id theft/ id fraud are
> used in the U.S. Here in the U.K [and in Australia] there is no
>> consensus on what constitutes id theft and whether or not it is
>> different to id fraud.
>>
>> Any help you could give me would be greatly appreciated.
>>
>> Regards
>> Tim Holmes
>> --
>> T.Holmes sop011@bangor.ac.uk
>>
>>
>
>

----- Original Message -----
From: <mmm151@pegasus.rutgers.edu>
To: "T.Holmes" <sop011@bangor.ac.uk>
Sent: Thursday, March 30, 2006 3:51 PM
Subject: Re: U.K ID FRAUD

> Hi again,
> It sounds like the issue has developed about the same as it has here, only
> we really didn't have one precipitating incident. In fact, it's like
> identity theft sprang out of the ground one day. What year was the Derek
> Bond incident by the way? I've never heard of it and I came up with a few
> thousand hits when I did a search.
>
> As you mention, id theft is linked over here with terrorism, illegal
> immigration, organized crime, benefits fraud, and the kitchen sink. I
> know the UK has been fighting over the issue of national identity cards
> for a while, and the first proposal for one over here appeared about 30
> years ago. The issue was resurrected after 9/11, with the obvious desire
> to fight terrorism, but this soon morphed into protection against identity
> theft and other social ills. The federal government has just passed the
> Real ID Act of 2005, which attempts to reform drivers licenses with the
> stated purpose of addressing illegal immigration, but their plan
> essentially creates a national ID card. Our government has also been
> fiddling around with their plan for Total Information Awareness (aka, Big
> Brother), and even though the plan was voted down several times, it keeps
> resurging in different forms. Whether they say so officially or not, the
> FBI/CIA and other agencies have been creating a national information
> database on its citizens, and they are in cahoots with private industries
> who routinely collect and sell our personal information.

>
> All of this has also been accompanied by claims that id theft is a growing
> menace and that is has become an epidemic, but of course there is no
> evidence (or only cooked evidence) to support such claims. I'm still
> trying to locate the origin of that one, but from what I can tell I right
> now it came from a New York or a California senator. Do you know what
> year this claim surfaced in the UK?
>
> Can you also give me the citation information for the Frank Nesbitt
> thesis? I'm basically looking at the same issue, but it's a bit more
> complicated in the US. It seems like the momentum of id theft was started
> by victim advocates, but I know the finaicial industries (particularly
> credit card companies) had a hand in it. The government was kind of slow
> to react, but there really is no separation between the government and
> private industries over here, and this is obvious in the laws that have
> since been passed in the so-called area of "consumer protection". I
> definately think that private industries have attempted to turn the
> collective lemons of their predicament into lemonade by selling insurance,
> paper shredders, etc, but it doesn't necessarily fit that they concocted
> the whole thing for that purpose. The federal government seems a more
> likely culprit in terms of their plans for total information awareness,
> but the issue of identity theft seems to predate their goal of world
> domination. At any rate, I'd really like to take a look at the Nesbitt
> thesis considering the connections. Hopefully, I'll get some answers I
> need in CA, but I'll let you know.
>
> Megan
>> Hello Megan
>>
>> As someone who can talk the ear off a donkey about id fraud [I live on a
>> farm so that's a provable statement!]I am glad to find someone who will
>> talk for hours about id fraud.
>>
>> I use the term id fraud more than id theft because id fraud is a term
>> that was first used in the U.K in 2000 in a paper by Mike Levi and
>> Gareth Jones [for a couple of years this was all the academic work I had
>> on the subject].
>> Since then there have been a few who have done work on the subject -
>>
>> Prof Martin Gill
>> m.gill@perpetuitygroup.com
>>
>> Dr Natasha Semmens
>> N.C.Semmens@sheffield.ac.uk
>>
>> Dr Emily Finch
>> E.Finch@uea.ac.uk
>>
>> As I mentioned before there is no consensus on what id theft or what id
>> fraud is. Most definitions vary on the grounds of duration of the crime

>> or on the scope of criminal activity covered by the terms id theft and
>> id fraud. What is clear is that id fraud has become a concern in the U.K
>> when discussing -Terrorism, use of the internet, illegal immigration
>> [within this are some forms of organised crime], fraud against the
>> credit industry and personal safety of U.K citizens. I have outlined
>> below some of the reasons for this -
>>
>> Id fraud was not a big issue in the U.K until the Derek Bond incident.
>> I don't know if you have heard of this case, an old man is thrown in a
>> South African jail for three weeks because someone was using his
>> identity in the U.S.A to commit crime. I do not know how much coverage
>> this case got in America but it was big here and it was such a big news
>> story that it kick started the news media's interest in people who had
>> lost their identity. Subsequent stories were not as big or shocking but
>> they did demonstrate that everyone was at risk, and the media made
>> point of showing how little people were aware of the risk they faced.
>> Recently we had another big id fraud case, this was a man who claimed to
>> be Lord Christopher Buckingham for 23 years when in fact Christopher
>> Buckingham had died as a baby. The man claiming to be Christopher
>> Buckingham gad built a life for himself with this identity. He had a
>> wife and two kids and a job as good job and had all the documentation
>> that the real Christopher Buckingham would have had. He was caught when
>> he used his passport on a trip back from France. There had been a
>> cross-referencing of passports with the register of deaths while the man
>> claiming to be Christopher Buckingham had been away. Further
>> investigation showed that he had stolen Christopher Buckingham's
>> identity and the man was imprisoned for two years for providing false
>> information on a passport application. What made the case even more
>> newsworthy was that the man refused to divulge his real identity. He
>> even denied his children when they asked to know who he really was. This
>> has lead some to speculate about why he refuse to divulge his real
>> identity. [I have digressed a bit, sorry, I told you I like talking
>> about this subject!!]
>>
>> The Derek Bond case got mixed up with the September 11th terrorist
>> attacks, concern over state benefit fraud and the rise in illegal
>> immigration in the U.K and created a national interest in finding out
>> who's who. The credit industry here has been very instrumental in
>> raising awareness of id fraud there is a group called the Credit
>> Industry Fraud Avoidance System [CIFAS www.cifas.org.uk] they and
others
>> from the credit industry have put forward this figure of 1.3billion
>> pounds per year lost because of id fraud. This figure pops up every
>> where in discussions of id fraud. CIFAS was also one of the first to
>> claim that id fraud was the fastest growing crime in the U.K. I read a
>> MA dissertation from a guy called Frank Nesbitt, he argues that the
>> phenomena of id fraud was constructed by the credit industry so they
>> could sell protection against id theft
>>
>>

>> The U.K government's response has been to create the National Identity
>> Fraud Unit which is a part of the Department for Works and Pensions.
>> They deal with fraud in the state benefit system and advise on how to
>> detect id fraud.
>>
>> The government also put forward the National Identity Card Scheme. One
>> of the key selling points the government put forward for the id card
>> [and the one my study looks at] is its use as a crime prevention tool.
>> Without much in the way of research or consensus on what id fraud is the
>> government has decided that the solution to id fraud was a
>> bio-metrically secure id card.
>>
>> Id cards are a big issue here, many are opposed to their introduction on
>> the grounds of civil liberties and right to privacy. What doesn't get
>> much attention is the practicalities of the system. People get hung up
>> on the question of whether or not we should have an id card that they
>> rarely stop to ask if it will work as a preventer of id fraud. The
>> London School of Economics has done some work which is critical of the
>> id card. There is a guy from the LSE called Simon Davies who has a web
>> site called Privacy International http://www.privacyinternational.org/
>>
>> Mostly when you talk about id fraud in the U.K the conversation usually
>> turns to id cards and vice versa. I am interested in looking at America
>> and Australia because my understanding is that id cards don't play much
>> of a part in discussions on id fraud. I am trying to see if there is an
>> alternative the U.K could use to id cards.
>>
>> If you are interested in international accounts of id fraud/id theft I
>> have found that the U.K, U.S.A and Australia are the only places that
>> are researching id fraud. I recently started talking to James Blindell
>> from the Australian Centre for Policing Research.
>>
>> I have to end this email know my fingers are starting to hurt
>>
>> Thanks for the help
>>
>> All the Best
>>
>> Tim
>> --
>> T.Holmes sop011@bangor.ac.uk
>>
>
>

----- Original Message -----
From: <mmm151@pegasus.rutgers.edu>
To: "T.Holmes" <sop011@bangor.ac.uk>
Sent: Wednesday, April 05, 2006 4:51 PM
Subject: Re: U.K ID FRAUD

> Hi Tim,
> Thanks for the info and the article on Derek Bond. My trip was
> informative to a degree, but I haven't quite figured out how the whole
> thing started yet. I'll be speaking with two more people next week, and
> will begin putting together a time line of the events I've learned about.
> It certainly seems at this point that private industries had a large role
> from the very beginning. It is also clear that the federal government has
> since passed weak preemtive legislation in favor of businesses
> (wishy-washy stuff that states must follow regardless of their own
> regional laws), so I'll have to do some more digging to figure out how
> they are involved. No one could really tell me when or why the term
> identity theft came to be used, but I'll keep you posted as I find out
> more.
> Megan
>
>> Hi
>> The Derek Bond incident was in 2003, his id was stolen 14 years before
>> his arrest by a man called Derek Lloyd Sykes. Sykes was a British man
>> living in Houston Texas where he was part of a telemarketing scam. In
>> 1999 Sykes [using Mr Bonds name] was indicted for money laundering, wire
>> fraud and transporting stolen property. This resulted in the F.B.I
>> issuing a warrant for the arrest of Derek Bond, when Mr Bond went on
>> holiday to South Africa he was arrested and put in jail for three weeks.
>> Meanwhile the F.B.I caught Sykes- now using the name Robert James Grant
>> in Las Vegas. This was a big deal in the U.K because Mr Bond was a 72
>> year old man who wasn't even aware his identity had been stolen and the
>> conditions in the South African jail were really bad.
>>
>> Frank Nesbitt is a police officer from Northumbria I can give you his
>> e-mail address, frank.nesbitt.1279@northumbria.pnn.police.uk
>> I am not sure if his dissertation is available except from Frank.
>>
>>
>> All the Best
>> Tim
>>
>> --
>> T.Holmes sop011@bangor.ac.uk
>>
>>
>
>

----- Original Message -----
From: <mmm151@pegasus.rutgers.edu>
To: "T.Holmes" <sop011@bangor.ac.uk>
Sent: Wednesday, April 26, 2006 8:29 PM
Subject: Re: Id Fraud

> Hi Tim,
> My holiday went well, thanks. I actually spent most of it coding data, so
> it sounds as if we both had a productive easter. Thanks for the info on
> KnightsBridge, I've never heard of them. I haven't heard the term
> "impersonation" per se, but I've seen several allusions to "The Great
> Imposter" - a book that was written in the 1950s and later become a movie
> in the 1960s. A similar term that I've seen used is "assumption". I
> actually prefer this term myself for different reasons, but there is no
> consistency in the literature. I've also heard the term "cloning" lately,
> but it is used in different ways.
>
> The situation in the US sounds similar to the one in the UK - it is not
> against the law to impersonate someone, but there is a fine line between
> impersonation and slander (which is still not identity theft). Its also
> not strictly against the law to possess the personal information of
> someone else, but it is against the law to steal it. I've done a little
> work on this aspect, because I think there has been much talk about
> stealing identities and not enough clarity regarding what exactly is being
> stolen. When I have those sections edited I'll send them to you.
>
> I personally think the issue of ownership is critical, although it
> receives little attention. The identity at stake in an identity theft
> is largely a social construction - pieces of information that are tied to
> my physical/emotional self. Much of that information has been bestowed
> upon me (my name, my social security number, my credit card number, etc.),
> but each is (in theory) a unique identifier of me - thus, now part of my
> identity. Imagine if one day banks or credit card companies claimed
> ownership over account numbers, saying they were theirs to do as they like
> with them. It wouldn't happen obviously because that number is now mine
> regardless of how it was assigned to me.
>
> Unfortunately, there are few controls regarding how corporations treat
> your personal information once it is given to them. Many companies sell
> information for a profit - but I don't make any money from it and I'm now
> beseiged by telemarkers and spam. If my identity were truly my own,
> however, companies would have to ask before sharing or selling my personal
> information. That would certainly be a start! I can't see any reason to
> give someone else the right to own or control the "personal information"
> that constitutes my identity - whether financial, emotional or physical.
> If I have to pay the ultimate price for its misuse, then I should have
> ultimate control over what is done with it.
>
> The answer to your question then is - whatever information is tied to me
> or used to identify me should rightfully belong to me (in my opinion).

> You can't separate a person's physical being from their social being, so
> you shouldn't be able to control social information at the potential
> expense of the physical person. I think the real answer though is that we
> NEED to claim ownership of it - it is certainly not being given to us.
> For me, it is a philosophical question - my identity reflects my existence
> and my rights in society. Many things are lost to expedience, but the
> only thing I can ever truly own in this world is myself. And if I start
> handing over the keys to the castle one by one, eventually I'll be locked
> out. Perhaps even more to the point - if I don't own my identity then who
> will? Who can I trust enough to manage my identity with my own interests
> in mind? - no one that I can think of.
>
> I'm babbling now, but this whole thing boils down to the control of
> physical identities as well - DNA tests, fingerprints, national id
> cards...etc. All of a sudden its against the law to dye your hair or wear
> colored contacts, then blood samples will be taken every time you board a
> plane or enter a government building; eventually we will have little chips
> implanted in us (instead of our id cards) so we can be scanned in a more
> orderly fashion. Ownership of information tidbits is how it begins, but
> it can very easily open the door to other forms of identity ownership and
> I say no to all of it.
>
> Hopefully, I haven't bored you with my rantings. I just don't think its
> fair (considering its intrinsic value to me and its market value on the
> street) that my identity should be up for grabs. I am interested though
> in hearing more about your views on national id cards and your impressions
> on the question of ownership.
>
> Megan
>
>
>
>> Hi
>> Hope you had a good easter, just got back after three week holiday [I
> say holiday, I spent three weeks shifting fire wood on the farm!] I have
> been searching the web and have come accross this group called Knights
> Bridge Castle. [http://www.knightsbridgecastle.com/index.html] Its a
> group that provides support for victims of identity theft in America, I
> mention them because I read somewhere on their website that they don't
> like the term id theft or id fraud becuase they don't believe that it is
> possible to steal somones identity. They have stories from victims of id
> theft where they said they prefer the term impersonation. Have you come
> accorss this distinction before in your work?
>>
>> I had not considered the issue of ownership that much in my work I
> acknowledge that everyone has an identity but can we claim ownership of
> it? In the U.K it is not illegal to use someone elses name or do an
> impersonation, for example when people impersonte celebrities like Elvis.
> At what point do you think we can claim to own an identity or what parts
> of an identity can be seen as exclusive to the legitmate holder of the

> identity?
>>
>> All the Best
>> Tim
>>
>> --
>> T.Holmes sop011@bangor.ac.uk
>>
>>
>> --
>> Gall y neges e-bost hon, ac unrhyw atodiadau a anfonwyd gyda hi, gynnwys
> deunydd cyfrinachol ac wedi eu bwriadu i'w defnyddio'n unig gan y sawl y
> cawsant eu cyfeirio ato (atynt). Os ydych wedi derbyn y neges e-bost hon
> trwy gamgymeriad, rhowch wybod i'r anfonwr ar
>> unwaith a dilëwch y neges. Os na fwriadwyd anfon y neges atoch chi,
> rhaid i chi beidio â defnyddio, cadw neu ddatgelu unrhyw wybodaeth a
> gynhwysir ynddi. Mae unrhyw farn neu safbwynt yn eiddo i'r sawl a'i
> hanfonodd yn unig ac nid yw o anghenraid yn cynrychioli barn
>> Prifysgol Cymru, Bangor. Nid yw Prifysgol Cymru, Bangor yn gwarantu bod
> y neges e-bost hon neu unrhyw atodiadau yn rhydd rhag firysau neu 100% yn
> ddiogel. Oni bai fod hyn wedi ei ddatgan yn uniongyrchol yn nhestun yr
> e-bost, nid bwriad y neges e-bost hon yw ffurfio contract rhwymol - mae
> rhestr o lofnodwyr awdurdodedig ar gael o Swyddfa
>> Cyllid Prifysgol Cymru, Bangor. www.bangor.ac.uk
>>
>> This email and any attachments may contain confidential material and is
> solely for the use of the intended recipient(s). If you have received
> this email in error, please notify the sender immediately and delete this
> email. If you are not the intended recipient(s), you must not use, retain
> or disclose any information contained in this email. Any views or
> opinions are solely those of the sender and do not necessarily
> represent those of the University of Wales, Bangor. The University of
> Wales, Bangor does not guarantee that this email or any attachments are
> free from viruses or 100% secure. Unless
>> expressly stated in the body of the text of the email, this email is not
> intended to form a binding contract - a list of authorised
>> signatories is available from the University of Wales, Bangor Finance
> Office. www.bangor.ac.uk
>>
>>
> > > > > > >

----- Original Message -----
From: rose300_williams@yahoo.co.jp
To: rose300_williams@yahoo.co.jp
Sent: Tuesday, December 04, 2007 10:02 PM
Subject: {Spam?} From miss williams

From: rose williams.
Abidjan Cote d' ivoire
West Africa.

Dearest One,
Good day to you.
My name is Miss rose williams and am 19 years old. Is my pleasure sending you this message. I am requesting you to go through it carefully and get back to me the soonest.
I am contactacting you for a business venture which I intend to establish in your country. Though we have not met before, I firmly believe, that you will not lead me astray after fervent prayers and fasting.
There is this huge amount of nine million five hundred thousand U.S dollars ($9.5m) which my late Father Mr. Albert wiliams deposited for me in a Security Company here in Abidjan before he was assassinated by unknown persons during the war in our country Cote d'ivoire. He intentionally deposited it as family valuables for its safe keeping in the Security Company.

Now, I have decided to invest this money in your country or anywhere safe enough outside Africa for security and political reasons. I want you to assist me claim and retrieve this fund from the Security Company and transfer it into your personal account in your country for investment. I will cheerish it if you can consider these listed areas below for the investment.

1). Telecommunication.
2). The Transport Industry.
3). Five Star Hotel.

I will be pleased and grateful offering you 20% of the total fund as compensation for your kind gesture and assistance.
God bless you and i await your soonest response.

Yours Faithfully,
Miss rose .williams

----- Original Message -----
From: Maria Stevens
To: mmaria_stevens70@yahoo.com
Sent: Monday, March 26, 2007 5:47 PM
Subject: {Spam?} My Dear Friend

My Dear Friend,

This letter might come to you as a surprise as we have not met before, but I believe that you would be compelled to help me after going through the contents of this letter. My name is Maria Del Carmen Stevens a swedish, my meeting with Mr David Yendall Stevens in south africa led us into marriage. my husband Mr David stevens who is now late farmer and exporter of Tobacco in the Republic of Zimbabwe, he was shot dead allegedly by ZANU-PF supporters in zimbabwe on 25th of april 2000 in the farm. You can confirm this by copying and pasting this link on your internet browser.or click on it:
http://news.bbc.co.uk/1/hi/world/africa/725643.stm,
http://news.bbc.co.uk/1/hi/world/africa/818766.stm

He (Robert Mugabe) did not stop at that; he also went on to expel all White farmers in Zimbabwe. He implored the services of his war veterans to undertake this seizure. The war veterans have been accused (correctly) of being behind the violent occupation of white-owned commercial farms in which an estimated 70,000 farm workers have been displaced. At least, over hundreds white farmers and black settlers have been killed since the farm invasions began in February 2000.We have decided that we must see this problem to the end.

Although we know that we are taking a great risk by staying here in Zimbabwe. At the Moment, our phone lines are bugged, and all our movements are being monitored by Zimbabwe's (Robert Mugabe)secret Police. Therefore email is the safest means of communication for now.
We (White farmers in Zimbabwe) have taken our case to the United Nations and even with the threats of transactions and the subsequent sanctions from the West against the Zimbabwean Authorities, Robert Mugabe (The president of Zimbabwe) still remains adamant.
He is insisting that our farm land (some of which we bought with our money and most of which We inherited from our fathers) belongs to the (his) government of Zimbabwe.the government of zimbabwe has asked all white-farmers to give up their farms to black farmers or risk going to prison. So far, more than 1,400 white owned farms have been invaded and confiscated, as well as claiming the properties of the farmers.Also, about 133 white farmers were arrested for defying the orders to leave their farms under the controversial land reform program of the government,

Since I could not keep the money in Zimbabwe, I used the services of a Diplomatic Courier Company to move this money (registered as official documents) out of Zimbabwe to Europe. At present, my money totaling US$28,750,000. (Twenty eight million, seven hundred and fifty thousand United States Dollars) is in Europe and hopefully, it would be paid into an offshore account. Can you help me? Are you trustworthy? Can you handle this money? Are you capable of handling this money? If you can, please contact me. All you need

to do is to claim this money from the Courier Company.

You will be required to contact the Courier Company that moved this money (official documents) out of Zimbabwe to Europe. All necessary particulars which can facilitate and enable you claim the money on my behalf will be forwarded to you as soon as your consent to proceed is received. For your assistance you will be entitled to have 20% of the total sum. You are also obliged to help/advise on the proper and most convenient way of investing this money in your country, Hopefully, You will consider this request and respond positively.

Yours Sincerely,
Maria Stevens

----- Original Message -----
From: "Mr. Paul Cooper" <paulcooper_1@katamail.com>
To: <sop011@bangor.ac.uk>
Sent: Saturday, June 30, 2007 8:37 PM
Subject: {SpamHigh?} Reply Asap...

> Hello,
>
> I AM MR Paul Cooper,A SOUTH AFRICAN working with SENEGAL BRANCH OF CREDIT MUTUAL DU SENEGAL AS THE MANAGER.My apologies if you find my mail intruding, i do not intend to offend you but only wish to use this medium to propose a business transaction to you which i believe would be of financial benefits to both of us if you agree to work with me.
>
> First,i would like you to know that i would understand if you take this proposal to be some scam or hoax as i would probably think the same in your place. I also receive a lot of spam mails all the time which to be honest with you is how i got the idea of contacting you through this medium from.I want to assure you this is a real and genuine business.
>
> I am sorry,i can only give you a few details of the transaction at this moment as i am not sure of your position yet and would not want to risk destroying everything i have worked hard for so far by being carefree and disclosing vital information's at this point that could get me into trouble,i have to be sure you are willing to work with me before i can give you the full details including my personal information's.
>
> The total amount involved is around NINE MILLION UNITED STATES OF AMERICA DOLLARS and all i need from you is to help me get the funds over to you safely, i have everything all worked out and there would be no risk or danger in this transaction.
> If you are willing to co-operate with me on this deal feel free to give me a call or write me ASAP indicating your sincere interest and for further information's and any questions you might wish to ask me. Thanks for your time and i look forward to a positive response from you soon.
>
> Thanks,
> Paul Cooper
> Email:p2cooper@box.az
> Telephone:+221-440-9966
>
>
>

----- Original Message -----
From: "Lesley Malone" <Lesley.Malone@victimsupport.org.uk>
To: <sop011@bangor.ac.uk>
Sent: Thursday, September 07, 2006 1:24 PM
Subject: RE: Study of Identity Theft

> Dear Tim
>
> Thank you for your email, and my apologies for not replying sooner.
>
> The statistical data that Victim Support collects shows the number of fraud victims we support, but does not unfortunately break the information down any further so it is not possible to tell whether these were victims of identity fraud/theft or other types. Fraud accounts for less than 1% of referrals to Victim Support overall, although it is part of our core service, (ie all Victim Support branches must offer a service to fraud victims). This means basically that information, practical help and emotional support as described in Victim Support's service model must be offered, to the specified standard, and branches must refer a victim on to another agency where they are better placed to offer the help or support required, and the person supported requests this.
>
> Just to touch on your point about victims approaching us - most victims are referred to us by the police when they report a crime, and the number of self-referrals we receive is very low (around 2%). We are also aware that although there is a formal agreement with the police that they should pass on details on all victims (except some agreed exceptions) that this does not always happen in practice, and it may be that victims of identity fraud who report it to the police are not always referred to us, for whatever reason.
>
> I hope this is useful - sorry not to be able to give you much information on this subject, but if you have any other questions about Victim Support's services or policies, I'll be happy to try and help.
>
> With best wishes
>
>
> Lesley Malone
> Information Officer, Victim Support National Office
>
> -----Original Message-----
> From: T.Holmes [mailto:sop011@bangor.ac.uk]
> Sent: 29 August 2006 14:12
> To: Reception Victim Support
> Subject: Study of Identity Theft
>
>
> Hello
> My name is Tim Holmes I am a PhD student at the University of Wales
> Bangor, I am conducting a study in to identity fraud. As part of my
> research I am trying to find out about victims of fraud. Can you help my

> study?
>
> I am trying to find out about what support and advice is offered to
> people who are victims of fraud and identity theft. Are there any
> statistics on the number of people who approach your organisation asking
> for help with regards to identity theft?
> Any help you could provide would be greatly appreciated.
>
> Regards
> Tim Holmes
>
> --
> T.Holmes sop011@bangor.ac.uk
>

----- Original Message -----
From: "enquiries" <enquiries@mi5.gov.uk>
To: <sop011@bangor.ac.uk>
Sent: Friday, March 30, 2007 4:36 PM
Subject: RE: English, Contact us

> Dear Mr Holmes,
>
> Thank you for your enquiry. Many of the targets of Service
> investigations have multiple identities, and any system that makes it
> more difficult for our targets to use and maintain multiple identities
> would be welcomed.
>
> The Home Office is the government department which is taking the lead on
> ID cards and you may wish to contact them directly at
> www.homeoffice.gov.uk/contact-us. Further information is available at
> www.homeoffice.gov.uk/passports-and-immigration/id-cards/?view=Standard
> and www.identitycards.gov.uk/index.asp.
>
> Good luck with your researches.
>
> Yours,
>
> Enquiries Team
> The Security Service
>
> This email has been generated from an administration account. Any
> replies will not be read. If you would like to send another message to
> the Security Service, please use the form on the website:
> www.mi5.gov.uk.
>
>
> Name
> Timothy Holmes
>
> Email
> sop011@bangor.ac.uk
>
> Message
> Hello
> My name is Timothy Holmes I am a criminologist from the University of
> Wales Bangor. I am conducting research in to identity cards and their
> possible impact on crimes sicu as identity fraud and terrorism.
> As part of my study I interested in the views of MI5 as to what
> impact/effect identit cards will have in terms of detection and
> prevention of terrorism.
> Any help you could give my study would be greatly appreciated.
> Regards
> Timothy Holmes
>