Debating the Technical & Ethical Limits of Secrecy & Privacy

Bakir, V.

Published: 24/03/2015

Publisher's PDF, also known as Version of record

PRIFYSGOL BANGOR UNIVERSITY

The University Of Sheffield.

Debating the Technical & Ethical Limits of Secrecy & Privacy

24th March 2015

E·S·R·C ECONOMIC & SOCIAL RESEARCH COUNCIL

Seminar Two: Summary

This summary is based on detailed notes from PhD students Abigail Blyth, Aberystwyth Univ.; George Petry, Univ. of South Wales; and Tiewtiwa Tanalekhapat, Aberystwyth Univ.

Introduction by Dr Vian Bakir and Dr Emma Briant: The seminar began with a summary of Seminar One on *Transparency Today: Exploring the Adequacy of Sur/Sous/Veillance Theory & Practice*, held at Bangor University and the role that Seminar Two plays within the series. Key was how to build on the theoretical first seminar by providing a grounded interpretation, highlighting the importance of cooperation between academia and end users' evidence through policy recommendations.

Ethical Limits of Secrecy and Privacy: Round-Table discussions

Steering Statement 1: A Conversation between Iain Bourne and Birgitta Jónsdóttir
Iain Bourne from the Information Commissioner's Office (ICO) spoke about the ICO's developing role, noting that even though they receive some 25,000 written complaints and 300,000 phone calls a year, very few of them relate to surveillance. Understandings of the connection between privacy, surveillance and security are therefore key as the relationship between how they interact with each other is largely confused.

Bourne also raised the problem of how to best understand the effect of surveillance on society, arguing that it is unclear as to whether increased surveillance has made the public less free to act as they might have wished. The idea of the surveillance state is changing as technology develops and how people use that technology changes. Interestingly, the ICO has expressed a desire to be partnered with academia, suggesting that other government departments are open to such collaboration.

Birgitta Jónsdóttir, as a poet, activist, political member of the Icelandic parliament (Pirate Party) and former Wikileaks volunteer, highlighted the significance and power of words and language and the role that we should all play in ensuring better communication. This included recognising the importance of freedom of speech and freedom of expression, as well as respect for the right to privacy and access to information. She urged us to move away from the dense techno-language of data usage towards something more meaningful for people. She ambitiously aims to raise public awareness and create a practical resolution on these issues at the Inter-Parliamentarian Union (IPU). Jónsdóttir was

therefore keen to understand how we can create a resolution with proper parameters that the IPU will be able to adopt as concrete guidelines.

Roundtable themes:

Perceptions, Understandings and Public Awareness: The importance of proper understanding of surveillance, and the damage from improper understandings, were a key theme for this roundtable. Birgitta Jónsdóttir noted that lack of public awareness meant that terminology was meaningless and that responsibility lay with the state to educate sufficiently before informed decisions can be made. Despite concerns relating to surveillance capabilities and arguments that freedom has been curtailed, more and more data is still put online. More analysis is needed on the effects this could have and how many citizens lack awareness due to insufficient education. The necessity for social scientists to be technologically educated is thus a key policy recommendation, but also needs to be broadened to include the wider public, policy makers and legislators.

Trust: Prof. Kirstie Ball spoke of how new measures, including integrity, benevolence, and competence, should be taken into consideration regarding the security-privacy relationship, both at state and citizen level if we are to understand the level and type of trust to be had for intelligence actors. Ball noted that the public might trust intelligence actors to be good at collecting data, but that there was a lack of trust regarding what they then did with it. With surveillance a part of everyday life, we need to ensure that there is proper oversight and transparency so that innocent civilians are not wrongly targeted. In the US, President Obama is seeking to do just this and although the Justice and Security Act of 2013 sought to provide the UK's Intelligence and Security Committee with more powers, there is still a need for more oversight of the intelligence community. It has taken some 19 years since the committee was established for its first meaningful report to be published. The roundtable concluded that public trust in the actions carried out by intelligence actors as well as the oversight process has been shaken. Colonel Ian Tunnicliffe who has previously worked with intelligence, said that while fictitious portrayals *sometimes* depict this realistically, on the whole they provide a distorted view of this work. This cultural representation, he argued, affects public trust, raising important questions regarding how to nurture trust when the secrecy of intelligence work might obscure the transparency by which we usually hope to ensure accountability.

Which Actors: Another key theme of the roundtable was the impact that private versus state surveillance would play. Tunnicliffe spoke of untangling the debate between different actors and targets. Allen Scott, from F-Secure (a company that makes software that protects people's data), argued that more is known about us than we know, especially by companies that hoover up data, such as Tesco, Google, Amazon and Yahoo. Important questions were raised regarding how different actors should be treated, and trusted, with our data and on what grounds we should base our analysis. Dr Madeline Carr suggested the significance of private sector and civil society representation, which can collaboratively work together to operate transparency.

Technical Limits of Secrecy and Privacy: Round-Table discussions

Steering Statement 2: Dr Steve Wright, Leeds Beckett University.
Wright historicised the debates around changing technological advances and illustrated the shifting focus of surveillance from one-to-one to one-to-many. A key focus was the discovery of the ECHELON signals intelligence and analysis network of the 'five eyes' states (US, UK, Australia, New Zealand, Canada and USA). He observed that while Watergate resulted in huge measures to increase oversight, post-Snowden there have been few measures to constrain hyper-surveillance. He observed a key advancement as the role played now by algorithms automating processes of data interpretation, which underpin military geo-location and dataveillance strategies. Modern surveillance has expanded capabilities for targeting, which can, of course, be applied for purposes more *or less* adherent to principles of 'social good' or democracy - principles which are in variance between different states. Wright expressed great concern that this targeting, even in the West, is moving further toward 'hunting uncooperative humans and then killing them' – highlighting the use of drones and other emergent technologies.

Roundtable themes:

Public responses to privacy and data management. One discussion focused on the public and its awareness and abilities in managing their privacy and their data online. Dr.Vian Bakir asked how permanent our data is online, and both Wright and Scott confirmed that nothing is ever truly deleted, leading to discussion of the implications of this permanent record. Jo Pierson also brought up how the obfuscation and hidden nature of the privacy controls mean that the public does not know how it is affected. There was mixed evidence of how concerned and aware the public is. Allen Scott (F-Secure) raised an experiment they carried out which evidenced people's naivety and trust in commercial systems. They placed free wi-fi hotspots outside the House of Commons and Canary Wharf. Even though the terms and conditions specified users agreed to give away their first-born child, 300 people signed up within 1/2 hour.

Future warfare and targeting. The discussion then moved to the revolutions in military technologies and future of warfare including an energised debate between Steve Wright, and Ian Tunnicliffe. Wright pointed to the advancement of US technologies toward a point where targeting and offensive weapons are able to take out cities with efficiency and speed. Though it is likely governments are exploring all possibilities for future defence, Tunnicliffe argued that future conflicts are to be the most observed conflicts ever, which mean civilian losses are increasingly unacceptable. The problem raised here is how combatants and/or 'enemies' are defined, as well as oversight and how proportionality is determined.

Limits for Researchers? Dr.Emma Briant raised the issue of the use of Google by researchers and surveillance of researchers. There may be a need for changing approaches to researching sensitive topics and a need for changing university practices for managing their communications.

Policy Recommendations

1. There is a need to raise technological awareness among members of the public, as well as for journalists and researchers to be technologically aware. As popular culture is often misleading in what it depicts, it may be helpful to develop 'creative' mediums to communicate surveillance issues and privacy tools reliably and effectively. This would ensure we are all more informed as well as reducing the 'trust deficit'.
2. With a proper process of application and review, universities should be able to allocate anonymised, secure research terminals to researchers and research students looking at sensitive topics.
3. There needs to be meaningful review of the oversight for surveillance in the UK as well as greater openness regarding the systems in place to ensure targeting is carried out in a way that protects minorities and respects free speech and civil/human rights. We must target incitement and planning of violent activities. However, *extreme views are not illegal*.
4. To improve oversight, and trust in this process, independent members of the public should be able to contribute to the Intelligence and Security Committee of Parliament.