‘This time with feeling?’ Assessing EU data governance implications of out of home appraisal based emotional AI

McStay, Andrew; Urquhart, Lachlan

First Monday

DOI:
10.5210/fm.v24i10.9457

Published: 07/10/2019

Peer reviewed version

This time with feeling? Assessing EU data governance implications of out of home appraisal based emotional AI by Andrew McStay and Lachlan Urquhart

Abstract

The boundaries of personal space and borders of bodily integrity are being tested by deployments of emotional artificial intelligence (EAI) in private and public spaces. By means of sensing, seeing and machine learning of facial expressions, voice, gaze, gestures and range of physiological signals (heart rate, skin conductivity and temperature, muscle activity, body temperature, respiration and other bio-signals), the goal is to make interior emotional life machine-readable for personal, commercial and security objectives.

In this paper, we focus on computer vision and face-based analytics to consider the nature, method and development of facial coding, the potential demise of existing approaches, and the rise of even more invasive methods. Criticisms of facial coding have long existed, but recent scholarship and industrial development signals a lack of confidence in 'basic emotions' and a turn to appraisal-based accounts of emotion. This inevitably entails use of data about internal physiological and experiential contexts, but also factors external to an individual. To explore this, this paper asks and answers the following question: With regard to deployment in out-of-home situations, what are the legal and privacy implications of appraisal-based emotion capture?

Introduction

The boundaries of personal space and borders of bodily integrity are being tested by deployments of emotional artificial intelligence (EAI) in public spaces. These enable intrusion into the hearts and minds of citizens by making psycho-physiological life visible. This is through gauging and machine learning of facial expressions, voice, gaze and gestures, and physiological seeing and sensing of blood flow, heart rate, body temperature and respiration, among measures. We unpack these new surveillance practices, raise concerns about how EAI impacts data privacy in public, and assess scope for accountability of EAI systems.

The widening ecosystem of actors bearing witness to intimate emotional details, interpreting and classifying citizens raises questions about the adequacy of regulatory controls for personal data and the inferences made. In this paper, we focus on situations where choice about the body and mind being read by EAI is much less clear, such as with emergent use of facial coding in public and civic spaces. To do this, we provide an overview of the technologies, detail ethical harms, map legal risks and outline socio-technical safeguards necessary for the emergence of publicly accountable emotion-sensing applications. We focus on machine learning, computer vision and face-based analytics to consider the nature, method and development of facial coding, and its potential demise. Criticisms have long existed, but recent scholarship and industrial insight signals a lack of confidence in 'basic emotions' and a turn to appraisal-based accounts of emotion. This paper asks and answers the following question: With regard to deployment in out-of-home situations, what are the legal and privacy implications of appraisal-based emotion capture?

Technologies that seek to learn and react to human emotions will be increasingly mainstream by the early 2020s (Gartner, 2018). This is emerging due to economic, organisational and personal value in recognising emotional and human state. In this paper we are particularly concerned about EAI entering public spaces where interactions and expectations of control over information collection and subsequent use can be harder to mediate. Paying special attention to out-of-home advertising and urban space sensing, which are linked in part to latent smart city initiatives, this paper is concerned about how EAI is entering everyday life. Currently, EAI poses many unanswered questions. These include how are different forms of EAI underpinned by computer vision making citizen feelings machine readable? Is the methodology sound and, if not, what are the consequences? Core to this paper is the question of what if they are becoming more reliable? As will be explored, while many current applications depend on digital derivatives of the Facial Action Coding System, an approach that has received heavy criticism, what if approaches more sensitive to internal physiological and social contexts were employed? This 'appraisal' based approach seems likely and to anticipate this, in this paper, we focus on implications of EAI in public from socio-technical, ethical and legal angles. Accordingly, we examine key provisions of the 2016 European General Data Protection Regulation (GDPR), the existing ePrivacy Directive 2002 — updated 2009 — (ePD) and a version of its proposed replacement the proposed ePrivacy Regulation (ePR) (which remains in a state of legislative flux).

Technical dimension of emotional AI: Facial action coding

The technologies in question derive from affective computing techniques and advances in machine learning and 'artificial intelligence' (AI). Taken together, McStay (2018) dubs these emotional AI (EAI). This is a weak form of AI in that these technologies aim to read and react to emotions through text, voice, computer vision and biometric sensing, but they do not have sentience or emotional states themselves. This weak, task-based, non-general and narrow form of AI is reliant on machine learning, a sub-domain of wider AI research (Cawsey, 1998). What is here termed EAI is a form of understanding based on simulation, rather than authentic experience (McStay, 2014). The simulation of understanding involves machine training and reading of words and images, seeing and sensing facial expressions, gaze direction, gestures and voice. It also encompasses machines sensing and learning about heart rate, body temperature, respiration and the electrical properties of our skin, among other bodily behaviours.

The key for modern industrial applications of EAI is that machine-learning techniques allow detection of patterns in known data to adapt to new data and thus the environment of deployment. In many cases of EAI, this will involve supervised machine learning (for example in the field of computer vision, where input training data is annotated/labelled by the trainer (e.g., picture of face 1 is 'happy'; picture of face 2 is 'sad') to develop a model that is able to detect outputs, and key features of those, when presented with new data. Often this provides a weighted finding of certainty of what is present (e.g., 73 percent certainty this photo shows a person who is 'happy'). At other times, unsupervised learning may be used where greater numbers of variables are present and there are multiple input training datasets. Instead, data is not labelled, as the output is not known. Rather, the system is delegated tasks of clustering or classifying features and making probabilistic

assessments about relationships between these. As a result, when presented with new data, machine learning systems make judgments about this fresh data without being explicitly told what is there.

In this paper's case, input features might be facial expressions, voice samples or biofeedback data and the output features are classified emotional states. In the case of faces, learning and adaption is often facilitated by use of convolutional neural nets. This is an approach to machine learning especially suitable for images because fewer connections within networks are employed to increase efficiency and reduce processing and storage (Altenberger and Lenz, 2018). Relatedly, region proposal networks show multiple objects identifiable within a particular image, allowing rapid detection and tracking of faces and other objects (Ren, et al., 2015). Finally, recurrent neural networks are used for audio and video processing. These are especially suitable for inputs that are sequences from time series prediction, video analysis, translating natural language or engaging in dialogue. Recurrent neural networks are neural networks that can be said to have a memory. Whereas feed-forward neural networks only consider the input it has been exposed to, the recurrent form draws upon the present input and those from the recent past, to determine how they respond to new data and how it should be labelled (Lipton, et al., 2015). In short, EAI pertains to understand a person's condition by means of how they are sensed, measured and remembered, as well as what rules are made for subsequent engagement with other people.

As will be developed, current "basic" means are problematic, yet the interest in seeing, reading, listening, classifying, learning and interacting with emotional life is socially significant. What is key is that emotional life is becoming machine-readable. Given historic and contemporary abuses of personal data, we suggest that EAI requires close critical attention.

The history of facial coding has practical origins in the nineteenth century with Duchenne (1990) who codified a wide range of facial expressions by detailing what muscles contribute to which named expression. Mention should also be made of Darwin (2009), who argued for a phylogenetic, autonomic and involuntary view of emotions because this sets the scene for the modern commercial belief that emotion capture provides authentic insights on emotion that self-reporting techniques miss. Today, computers attribute pixels to facial features to register emotional behaviour. This includes faces from camera feeds, recorded video files and photos. Although facial coding applications acknowledge dimensional approaches to emotions by measuring valence (the pleasantness continuum) and how aroused a person is, it is premised on a categorical approach to emotions (i.e., labelling emotions into categories e.g., anger, contempt, disgust, fear, happiness, neutral, sadness, and surprise) and there being a suite of basic emotions (McDuff and el Kaliouby, 2017). It is also grounded in the premise of reverse inference, where expressions reveal information about a person's emotional state that cannot be accessed directly (Barrett, et al., 2019).

Non-specialists should note that the universalising, categorical and basic emotions worldview has long been subject to sustained methodological critique for being Western-centric. This is exemplified in Ekman and Friesen's (1971) landmark study in the New Guinea Highlands, and responses to it. At the time of Ekman and Friesen's study, inhabitants of the Highlands had not been significantly

exposed to advanced media systems, television and photographs of people's faces from other countries. By studying people and facial expressions in different cultural contexts to the West, and finding commonalities with Westerners, Ekman and Friesen concluded that emotions and facial behaviours are universal. However, Russell (1994) queries the hypothesis, method, findings, classification of findings, testing procedures, level of exposure to Western discourse, and degree of experimental control in this cross-cultural work. For example, Ekman and Friesen did not speak the local language, which in turn meant there was use of translators. This resulted in a lack of ability to monitor what was being said and the potential influencing of test subjects by the translator, who could not be expected to appreciate the need for an untainted study. Russell also quotes Sorenson (1976) who was present at the study itself, who said that the pictures and procedures were the subject of active interest and discussion by the behaviourally alert locals, and that they were sensitive to subtle cues about how they should respond and react. This analysis led Russell (1994) to argue that the evidence is not a good enough to conclude that emotions and display behaviour are universal (McStay, et al., 2019).

Nevertheless, the Facial Action Coding System (FACS), the measuring of facial movement in humans and the refining of a taxonomy of human emotions and facial expressions was developed (Ekman and Friesen, 1978). FACS is based on Ekman and Friesen's identification of seven facial expressions of primary emotion (joy, surprise, sadness, anger, fear, disgust and contempt); three overall sentiments (positive, negative, and neutral), advanced emotions (such as frustration and confusion) and 19 Action Units (AUs). Today's approach uses computer vision techniques to code combinations of facial movement to arrive at interpretations of emotional categories and states. These typically work by tracking muscles and moments around the mouth, nose and eyes. Affective computing technology is well developed in that it reacts in real-time to facial movement for a variety of emotions. For example, it discerns between quick reactive smiles (as with outbursts of laughter) or longer periods of amusement (such as with dark comedy). This is recognised by movement of lip corners, the speed with which this occurs and the length of time the corners are moved from their usual position. Nose wrinkling represents emotions such as disgust, and depressions of the corner of lips are connected with sadness.

As noted, in addition to clustering facial movements into emotion types, emotions are also judged by a dimensional valence score to provide understanding of whether the emotion is positive, neutral or negative. They are also modelled by arousal and whether a person is bored (or even asleep) or if they are frantically excited. Another measure is power, or the extent to which they have control over the emotion (Gunes and Pantic, 2010). Thus, while proponents of categorical approaches do not fully answer Russell's (1994) ethnocentric criticisms, they embrace measurable dimensional factors to triangulate and strengthen conclusions about the extent to which a person is undergoing a named emotion.

Methodological problems with this approach have long been understood, but they have been empirically demonstrated by Barrett, et al. (2019) who point out that the basic emotions approach does not capture how people convey, or interpret, emotion on faces (for example, a smile can express more than one emotion depending on the situation, the individual, or the culture). Given that 'similar configurations of facial movements variably express instances of more than one

emotion category' (Barrett, et al., 2019), what is clear is that more detail on the context of the situation is required to understand the emotion.

Scholars, critics and even industry are beginning to see that for the emotional AI sector to grow, it must relinquish its usage of basic emotions approaches that are too crude to comprehend emotions. Industry is aware that basic approaches are problematic but, arguably, the lure of an approach to emotional life that works well with existing computer vision technology has meant that methodological errors have been wilfully overlooked (McStay, 2018). Microsoft for example point out in a peer-reviewed publication that: 'only a very small number of behaviours are universally interpretable (and even those theories have been vigorously debated). It is likely that a hybrid dimensional-appraisal model will be the most useful approach' [1].

On one hand this is positive, especially given critiques of bias, phrenology, lack of admission of social context, and that emotion has a social as well expressive function. However, a turn to context will inevitably involve a turn to data, especially in quasi-private "smart" spaces. Basic emotion approaches to face-based emotional AI are coming under critique for over-simplicity and reliance on core prototypical facial configurations that "reveal" an emotional state (Barrett, et al., 2019). We argue that this will prompt an industrial pivot to more appraisal-based approaches that admit of the temporospatial context in which a facial expression is recorded. This is not straightforward, with Microsoft stating that 'there are no commercially available software tools for recognizing emotion (either from verbal or nonverbal modalities) that use an appraisal-based model of emotion'. However, the trajectory of the EAI industry is made clear by the follow-up statement: 'Incorporating context and personalization into assessment of the emotional state of an individual is arguably the next big technical and design challenge for commercial software systems that wish to recognize the emotion of a user' [2]. By applying Barrett, et al.'s (2019) critique, we can anticipate appraisal-based EAI will involve the connection of facial movements with internal and external contexts: a person's internal context will involve metabolic and experiential dimensions; and the outward context factors such as regional and societal norms on emoting, specifics of the situation (e.g., is a person at home, school, work, in the car), and social factors (who else is present).

The value and means by which the turn to context will occur is clear, it will involve: 1) invasive (involving physically touching a person) and non-invasive sensors (such as use of remote cameras to gauge internal states such as heart rate) registering of affective and metabolic states; 2) use of devices and profiling of services (such as data from smartphones and social media); 3) ambient awareness of context (such as weather, place, location, footfall and other factors unique to the socio-spatial character of the place in which emoting is taking place).

Emotional AI in public

Sectors, surveillance techniques and reasons for interest in machine-readable emotions are highly diverse, but each is conjoined by an interest in gauging authentic emotional reactions to circumstances. As smart city initiatives are guided by the rhetoric of changing cities into efficient,

well managed, user aware spaces, emotional AI could play a key role in emergent smart infrastructures (Shepard, 2011; McStay, 2017; Urquhart, Schnädelbach and Jäger, 2019). In London 2015 for example the advertising agency M&C Saatchi (partnering with Clear Channel and Posterscope) produced an ad that evolves unique ads based on people's facial reactions. This entails analysis of audience emotions as people move throughout public spaces (McStay, 2016). Others, such as Ocean Outdoor, a U.K. out-of-home advertising company, also target by age, gender and geolocation and have used emotion tracking. The most prominent example, beginning in London 2017, is significant because of its scale. Involving a screen in Piccadilly Circus the size of four tennis courts, Ocean Outdoor and the site owners Landsec, analyse expressions of pedestrians to assess facial reactions and customise future content. Cameras also analyse age and gender of passers-by, as well as the manufacturer, model and colour of cars passing through the gaze of cameras [3].

In retail, SBXL, a U.K. retail analytics firm, use facial analytics in leading retailers such as B&Q (a hardware and garden store), Boots, TK Maxx and Tesco [4]. The scope of emotional AI to exponentially scale is best appreciated by recognising that leading facial recognition systems are also bundled with emotional AI (for example Amazon's AWS Rekognition [5] and Google Vision [6]). This sees EAI as a layer that complements other applications, as opposed to a standalone product. Although this paper focuses on facial analytics and urban experience, closely related are use of face-based emotional AI for in car experience and safety telemetry, entertainment and empathic interactions (Topham, 2018). Similarly, workplace analytics also exist, using computer vision to measure 'employee attitude and engagement continuously and passively ... through emotional analytics of shared spaces and video meetings' (Sensing Feeling, 2018).

Ethical harms, concerns and challenges

In so-called "smart cities", there is a potential mismatch between the values of those who live there, the market led logic of those providing infrastructure (Greenfield, 2013; Kitchin, 2014) and significant scope for privacy harms (Edwards, 2016). Emotional AI, especially appraisal-based methods, amplifies these concerns, as it sits as a layer within other smart city services. In this section we introduce some of the key challenges to be addressed so more trustworthy, legally compliant, ethically sound emotional AI can emerge.

Loss of ephemerality: EAI enables a shift from emotive states being transient and ephemeral to becoming datafied, catalogued, scored and potentially retrospectively assessed. Control over who gets to audit, access and interpret such records over time depends on affordances of the system for user oversight, and practices of the service provider. Context can be lost when data is viewed a long time after it has been initially collected, which enables different interpretations of the data. The virtues of analogue forgetting, such as partiality or fragmentation of memories, are at risk here (Mayer-Schönberger, 2009; Dodge and Kitchin, 2007), particularly when EAI ties into emotion, an inherently intimate domain of human life. As EAI is embedded in public infrastructure, this enables new interactions with the built environment over time. We need to begin to think more longitudinally not just in terms of users' or device lifespans, but of buildings. This requires greater

attention from interaction designers and architects to ensure human building interactions respect needs of users and good data governance (Urquhart, Schnädelbach and Jäger, 2019).

Manipulation: There is scope for harms at the point of both sensing initial data, but also in how EAI affects users and shapes their behaviour (Fogg, 2012). How EAI is used in public spaces, perhaps to encourage purchasing of new products in retail, is problematic (Turow, 2017; McStay, 2016). While retail spaces have historically been designed and optimised to nudge and elicit consumption, the act of sensing, registering and reacting to in-store emotional behaviour is more intrusive than store feature design and footfall tracking. The future of manipulation has echoes of what in design for Web and mobile apps is referred to as 'dark design' (Forbrukerrådet, 2018). For EAI, the impacts of design decisions that involve manipulation, deceit, erosion of trust, exploitative nudging, misleading consumers or denying choice can be both more effective and affective.

From a governance perspective, it is important to learn lessons from the Web space, to ensure such manipulation, price differentiation and perceptions of targeting do not come to dominate EAI applications embedded in the physical spaces of everyday life too. More innovative approaches to designing consent mechanisms in retail, for example, will be needed, especially given interest in 'user experience' and their anticipated 'trajectory' through stores (Urquhart and Rodden, 2017).

Resistance: As emotion and affective states become computationally visible, it will be difficult for individuals to exercise resistance to observation and monitoring. For example, how would Gary Marx's strategies of surveillance resistance apply in public spaces (Marx, 2003) such as to discover, avoid or counter surveillance? As Marx argues, resistance is often a game of cat and mouse where the watched and watcher "continually learn from each other and reiteratively adjust their behaviour in the face of new offensive and defensive means" [7]. Greater transparency about how the body is read by EAI could enable resistance by subjects. However, 'hiding' emotions, where metrics like heart rate or facial movements are used in conjunction with contextual variables means resisting appraisal based EAI may be harder than just masking the face, as has been one response for facial recognition, for example (Monahan, 2015).

Furthermore, the distributed nature of data collection in public space means it is not one actor or disciplinary entity citizens need to contend with but a complex assemblage of actors (Deleuze, 1992; Haggerty and Ericson, 2000) from retailers and councils to transport firms and police. Hence, when EAI can be used for social control in urban spaces to such an extent that it could become hard to even avoid the ambient data collection infrastructure (Graham, 2009; McStay, 2017; Schnadelbach, Jager and Urquhart, 2019), the question of 'if resistance is futile?' becomes pertinent to ask (Fernandez and Huey, 2009).

Impact on identity: By making emotion visible, this may impact the space left for individuals to formulate self-conceptions and identities, a key aspect of privacy (Solove, 2006). This is the issue of the constitutive and unnatural role of technology that technology is beginning to play in co-shaping perceptions and understandings of emotion. As Verbeek (drawing on Don Idhe) explores in relation

to technological intentionality, mediating technologies 'amplify aspects of reality while reducing other aspects' [8], which means that they inform what counts as real. Looking forward, as emotion detection is developing through changes in psychological methods (i.e., appraisal-based), new sensing methods (more contextual data points) and novel data analytics techniques. Thus we will continue to need to scrutinise where "knowledge" about emotion emerges from, and what the consequences are when people apply knowledge constructions to their own identity. As discussed above, on basic emotions, to date these constructions have served particular commercial interests. Relatedly, they have also served technology development interests due to wilful overlooking of: a) limitations of sensing technologies; and b) understanding of what emotions actually are (those leading start-ups and corporate research facilities are aware of the limitations of basic emotions, often possessing doctorates in relevant topics). This raises the issue of whether we are reducing emotional life to what can be measured. The legal and socio-political concern is that poor constructions of emotional life may have material consequences for how decisions are made about us in retail, advertising, automotive, workplaces, and many other life contexts (McStay, 2018).

Uncertainty: EAI involves categorising features into groups and classifying affective states through a process of emotional sorting. As Lyon (2003) argues, social sorting of populations is a form of surveillance which can lead to harm as individuals are categorised and treated differently as a result. We extend this idea, arguing emotional sorting attempts to make emotional states visible, using these for inferences and knowledge about human states otherwise invisible to computation. Holding these inferences to account involves not just challenging data gathering practices, but also understanding and critiquing models of emotion detection.

In metricising emotions and making them machine readable, there are clear risks in managing decisions based on these assumptions. The causal leap from presence of physiological markers (such as micro-expressions) to claims of a particular emotive state (such as angry, happy or sad) risks unfair, pre-emptive treatment of citizens. This is amplified by lack of academic agreement about what emotions actually are. Scientific debate remains about what is being seen by EAI (Martinez, et al., 2017) but different contexts of use may result in significant, legally actionable harms. For example, within law enforcement, EAI data would be valuable in predictive policing and, similarly, in situ assessment for insurance could shape claims processes e.g., in-car reactivity and perceived recklessness from smart rear-view mirrors detecting 'road rage'. This sits against a wider backdrop of technological approaches to read individual attributes from physiological markers, for example the neo-Lombrosian trend of trying to predict criminality not from phrenology, but instead from machine learning on facial features (Wu and Zhang, 2017).

The governance of emotional AI

Having broached ethical concerns, we now turn to more focused discussion of governing EAI, especially in light of the demise of "basic" approaches and anticipated rise of "appraisal"–based approaches to EAI that functions in relation to facial expressions. In responding to EAI governance in public there are two legal frameworks, namely, the EU General Data Protection Regulation 2016 — GDPR) and the current EU ePrivacy Directive — EPD — and the proposed replacement Regulation —

EPR) [9]. Firstly though, we consider the challenges posed by fragmented regulation of this new domain.

Fragmented regulation

We have concerns about the fragmentation of regulation arising from differing deployment settings for EAI. As we see below, how and where emotion is sensed is one factor that can dictate when and which legal framework applies. For example, where may depend on if a reasonable expectation to privacy exists or not in the public, semi public or private space (where the parameters are not always clear — e.g., train stations/airports/shopping centres). For how, if the EAI system uses a public telecoms or private network to communicate data, this shapes the applicability of the law because systems using private networks may fall outside the scope of the EPD (Edwards, 2016). Similarly, it matters who is operating EAI systems and why. If data processing is conducted by relevant law enforcement agencies (e.g., police), there are GDPR exemptions when processing is for the prevention and detection of crime (Art 2(2)(d), GDPR), and instead the EU Law Enforcement Directive (2016/680) could apply. However, assessing when either framework applies would be difficult as many cases of public space surveillance involve outsourcing or partnership with private organisations. Beyond DP law, use of public surveillance by law enforcement raises questions about 'reasonable expectations to privacy in public spaces' (Edwards and Urquhart, 2016). We see this with recent court cases about police trials using facial recognition (FR) (R [Bridges] v Chief Constable of South Wales Police and Secretary of State for the Home Department, 2019). This sits against the legal backdrop that even taking photos in public for further use by police, without the subject knowing why and what they are for, can interfere with Article 8(1) of the European Convention on Human Rights (R v. Commissioner of Police for the Met [2012] EWHC 1681; Law Society, 2019). That said, in this article we foreground data protection concerns in the commercial/civil sector (as opposed to law enforcement use).

GDPR: EAI testing established data protection principles

The GDPR contains a wide spectrum of data subject rights to help citizens control personal data processing. Even with personal data processing in public spaces, data subjects can approach controllers to access, correct, port and erase their personal data, in addition to restricting and objecting to its processing (Arts 15–21 GDPR). Public EAI challenges realisation of these rights by seeking to illuminate and influence our hearts, minds and intentions by ambiently reading bodily information. It is practically hard to control collection and interpretation of such information, but more fundamentally, there is uncertainty about if the GDPR definition of personal data captures emotion data (Clifford, 2017). Personal data (PD) is any 'information relating to an identified or identifiable natural person' (Art 4(1), GDPR), and if it is not PD being processed, GDPR does not apply. Assuming no other data to 'single out' is being used, McStay argues that EAI approaches using computer vision (CV) to gauge positive and negative expressions, or a wider suite of basic emotion expressions, may not be classifiable as personal data, because they do not aim to single an individual out (McStay, 2016).

Formerly, U.K. case law on PD narrowed the 'relating to' provision to only when there was a 'focus' on the data subject or biographical data 'relating' to them being collected (Durant v Financial Services Authority [2003] Civ 1746). Thus, with public space video (like CCTV) this meant operators could argue general footage of a public space was not PD relating to those passers-by, unless they became the focus of the footage e.g., by subsequent monitoring or examination by the controller (Edwards, 2004). However, subsequent case law challenged this narrow framing of PD (Edem v Information Commissioner [2014] EWCA Civ 92) and now under the harmonised GDPR, a broad interpretation of PD is now required [10]. Indeed, if we look to the U.K. Information Commissioner Office (ICO) guidance on CCTV, it states "the majority of surveillance systems are used to monitor or record the activities of individuals, or both. As such they process individuals' information — their personal data ... [and the code also covers] other systems that capture information of identifiable individuals or information relating to individuals." [11]. The significance of this is such controllers are subject to GDPR.

A key point to remember too, is subjects can just be identifiable, directly or indirectly, as opposed to already identified. Thus, there are faces of natural persons in footage which could be identified, even if this is not the purpose of processing, by addition of other data that singles out an individual. For appraisal-based systems, EAI operators will be more likely to combine data that could see them processing PD.

Processing under GDPR, whilst broad, always pertains to action (such as collection, recording, storage, etc.) with personal data (Art 4(2), GDPR). Some EAI systems only analyse footage in real time, which is not stored, but this would still not preclude being deemed processing, because recording and collection is included in the definition. In relation to FR, the ICO is quite clear that "any organisation using software that can recognise a face amongst a crowd then scan large databases of people to check for a match in a matter of seconds, is processing personal data." [12]

The business model of EAI firms is key here, as whilst their technology may not seek to single out individuals, they might still process personal data, or have legal obligations in handling audio-visual footage. What is the supply chain of the footage for EAI facial CV analysis and, with respect to purposes of processing, who sources footage, and what is the relationship is between sources of footage and EAI firms? Are firms providing the entire infrastructure, where they install cameras, collect and then analyse footage 'in house'; or do they source footage from third party operators and then provide a layer of emotional analytics for existing services? This is important, as the legalities of repurposing third party content will turn on lawfulness of that processing. What basis was the original collection based on, and is the repurposing still lawful under Art 6(4) GDPR? This involves considering the context of collection (including the relationship between the subject and controller; the link between the original purposes and further uses, but importantly, the consequences of further processing and if there are appropriate safeguards in place). The EAI firm still needs lawful basis for PD handling, and may even need to provide information about processing to subjects too, if feasible [13]. This is going to be a particular issue for access to training datasets, and who mediates access to these.

With new EAI deployments as a layer within existing camera systems or standalone full stack development (e.g., in retail), this could pose 'high risks to rights and freedoms of natural persons', and involve 'systematic monitoring of a publicly accessible area on a large scale' (Art 35(1) and (3), GDPR). As such, a data protection impact assessment would be required, to assess risks, likelihood of occurrence, appropriate safeguards and challenges of implementing these (Art 35(7), GDPR).

Furthermore, appraisal-based approaches, involving a mosaic of sensed contextual information (in addition to any CV facial analysis), thus it will likely involve subject identification. The controller will have access to data to identify directly or indirectly. They are more likely to involve personal data, because of need to understand internal (metabolic and experiential) and external contexts of a subject (including personal devices, outside of a person — so information and identifiers from smart phones and wearables). This introduces additional devices/services and data controllers, arguably with more scope to control data collection than with CV based data (e.g., switch off location services or Bluetooth on the phone etc.). Privacy is ensuring the contextual appropriateness of flows of information, where privacy harms stem from breach of integrity of those flows (Nissenbaum, 2010). Thus, systems which link or create new flows need to be queried for potential information privacy concerns.

However, as the PD definition shows, the legal framework in Europe still focuses on risks and harms from identification. Public concern around identification by facial recognition (FR) cameras in public has led to outcry at trials by police (Davies, et al., 2018), calls for stricter regulation at U.K. level (Wiles, 2019), polls of public opinion (Ada Lovelace Institute, 2019) and some scholars even proposing a moratorium on use of such technology (Crawford, 2019). However, we argue EAI goes a step further than FR, as it may not focus on identification of an individual, but instead on their intention. As the law is not as well placed to deal with controlling inferences about intention (as we see below with discussion on biometric data and data portability) this shift from identification to intention-based harms is quite profound for citizens. Accordingly, we need to consider how best to regulate non-identifying harms (and perhaps turn to wider privacy jurisprudence here), given the DP law may not provide all the safeguards.

As mentioned above, the Right to Data Portability (Art 20, GDPR) seeks to empower citizens to receive their personal data from controllers and transmit it to another controller (or store and manage on their own 'edge computing' devices for personal information management). The emergence of EAI means control of 'raw' data may only be half the picture in that citizen rights requiring increased control over their emotional profiles and how they are interpreted by organisations is not clear. The right to data portability (Art 20, GDPR) does not apply for derived/statistical inferences drawn from data analysis, a significant shortcoming for user rights when EAI relies upon inferences (Urquhart, Sailaja and McAuley, 2018). Indeed, the privacy harms may stem not only from the storage of metrics used to read the face or emotional state, but instead the inferences made on these such as if someone is sad or angry. This is increasingly important, as the causal link between presence of facial features (say scowling) and emotional state (say anger), is scientifically contested (Barrett, et al., 2019). What does this mean for notions of controllers maintaining accurate data in (Art 5(1)(d) GDPR), where the system may be working as intended, but the science underpinning the inferences is unsettled, challenging accuracy in the real sense.

Another element of control is ensuring the legality of data processing in public spaces, namely what are the legal grounds for data processing? There are numerous grounds, ranging from consent and fulfilling a contract to providing a service requested by the user and legitimate interests of the controller (Art 6(1), GDPR). To understand which applies, we first need to briefly unpack the discussion around if emotion data is biometric data, because if it is, processing will require the explicit consent of the data subject (Art 9, GDPR). Data concerning health, particularly mental health (art 4(15) could conceivably be read from facial coding (e.g., see work of Song, et al. [2018] on detecting depression using CV), and thus require, we argue requires explicit consent.

Biometric data is "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data" (emphasis added — Art 4(14), GDPR). As mentioned above, often with EAI, despite use of specific technical processing, it is not about identifying an individual to confirm/authenticate them for a service. Also, the video footage itself is not considered biometric (Recital 51, GDPR). Cameras may detect a face and analyze its state against an emotional model, but not identify it. This is analogous to the distinction between client-based face detection software in phone cameras that do not identify the individual, just recognizing a face, in contrast to a facial recognition system which would identify by checking those images against a database.

In trying to navigate the parameters of Art 9 for the EAI context, the EDPB argue, that if shop owners customizing ads using camera captured age/gender do 'not generate biometric templates in order to uniquely identify persons but instead just detects those physical characteristics and consequently only classifies the person, then the processing would not fall under Article 9.' [14]

This narrow focus on confirmation and identification in Art 9 neglects the harms of being watched by EAI (and possible scope creep as it is assimilated as a layer in combination with other surveillance systems). As the European Data Protection Board (EDPB) states, the purpose of processing must be to uniquely identify using the data [15]. It also states that when processing is used to distinguish categories of people, but not uniquely identify, it is not biometric data [16]. Indeed, identification could occur by a controller, depending on contextual personal data sought in appraisal-based systems. However, the standalone narrow framing of biometric data appears to offer little immediate recourse for CV based EAI, unless it is used for unique identification.

Legitimate interests could be one of the grounds for processing EAI data and whilst it is vaguely framed in the law, it has limitations. It cannot just be used for any processing that is in the economic interests of the controller, and instead they need to consider fundamental rights of data subjects (Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, 2014). Indeed, the EDPB, argue a 'real and hazardous' situation, that is not 'fictional or speculative,' may justify a legitimate interest for video surveillance, particularly where there is imminent danger [17]. This shows a high threshold, where: a) necessity must be shown of the need for such processing; and b) interests of the controller and subject have to be balanced on a case by

case basis looking at 'intensity of the intervention', impacting subjects. This can include factors such as the area and extent being monitored, in addition to if an objective third party would reasonably expect monitoring to be taking place or not [18].

Furthermore, context may come to dictate where EAI deployments are socially, and legally acceptable. For example, the EDPB [19] recently stated — "Data subjects can also expect to be free of monitoring within public areas especially if those public areas are typically used for recovery, regeneration, and leisure activities as well as in places where individuals stay and/or communicate, such as sitting areas, tables in restaurants, parks, cinemas and fitness facilities. Here the legitimate interests or rights and freedoms of the data subject will often override the controller's legitimate interests." [20] In the context of EAI for public advertising then, it becomes increasingly hard to argue it falls under the remit of legitimate interests (U.K. Information Commissioner Office (ICO), 2019c).

One legal ground that poses concerns for public space EAI, if personal data is processed, is consent. Ordinarily, gathering the requisite level of consent in public spaces for EAI is difficult, general, the requirements for consent are that it is freely given, specific, informed, unambiguous indication of the data subject's wishes (Art 4(11); Art 7; Art 8; Art 9 GDPR).

This requires that data subjects have information about what they have agreed to; that it has not been provided under duress or undue persuasion; that it is for specific purposes/uses; that it is an actual act or statement made by the subject, not just their silence taken as acquiesce. It also should be withdrawable and provable (as being recorded in writing, orally or electronically). Thus, it is quite a high threshold and set of design and compliance requirements for public EAI operators, particularly as appraisal based EAI may require consent mechanisms across a number of data controllers and devices. We return to consider consent below.

ePrivacy: Sensing emotions

The final form of the ePrivacy Regulation (and its legislative schedule — EU Parliament [2019]) remain uncertain. Nevertheless the 2017 European Commission ePR proposal indicates the direction of policy travel, if not the final wording. Some provisions may be removed, and already, there are reports of lack of agreement on wording (Council of European Union, 2018). We refer to both the current and proposed law here, where relevant.

In general, when there is a more specific rule in ePrivacy, this takes precedence over the general rule in GDPR (as per 'lex specialis') (EDPB, 2019b). The ePR harmonises consent requirements with GDPR definitions, as does the ePD which requires consent to the same standard as GDPR [21]. Thus, the Art 5(3) ePrivacy rule may take precedence over Art 6 processing grounds in GDPR. If information on a user's terminal equipment is personal data, prior consent is needed if a controller wants to store or access data there (meaning other grounds of processing, like legitimate interests, cannot count) [22].

Type of sensing: As basic emotion approaches to face-based emotional AI come under critique (Barrett, et al., 2019), we believe there will be a pivot to more appraisal-based approaches that require sensing and tracking of the context in which a facial expression is recorded.

This would entail both on-body and remote sensing for spatial and personal information. On-body could include device IDs, accelerometer or gyroscopic data on phones, location data and special categories of data (such as 'health related data' like heart rate from wearables).

With remote sensors, this could include infrared detection of presence, temperature and gait. Location data that does not identify the individual is covered by ePD rules which stipulate it cannot be used unless it is anonymised or it is necessary for a consented to 'value added service' (Art 9, EPD). Value added services vary but includes services like 'route guidance, traffic information, weather forecasts and tourist information' (Recital 18, GDPR). As an emergent market, it is interesting to consider what an EAI value added service might look like — perhaps navigating users through different routes, depending on how they feel (depending on the number and type of shops, restaurants or bars associated with the route). The ePD is broader than GDPR because it is not constrained to personal data. However, location data that is also personal data, may be captured by GDPR too (Art 4(1), GDPR) and both ePrivacy and GDPR can apply to the same processing activities [23].

Terminal equipment: Under the current ePD, as updated in 2009, prior informed consent is needed for information to be stored or accessed on the networked 'terminal equipment' of a user (Art 5(3), ePD). With the 'terminal equipment' the law envisages devices like smart phones, laptops and personal wearables. However, EAI sensing may not always be via a networked device. For example, basic EAI does not involve terminal equipment to track a subject (unless someone is an 'everyday cyborg' (Quigley and Ayihongbe, 2018) with networked equipment embedded in their body e.g., bionic eye, smart pacemaker or insulin pump). Furthermore, often the device will not pertain to an individual user but collect information from groups and many passers-by in public space. This shared computational infrastructure was a key shift in the growth from mainframe to personal to ubiquitous computing, a trend recognised as early as the 1990s (Grudin, 1990). Yet, data protection still generally focuses on personal data in terms of individual rights and harms, but is less adept at dealing with collaborative systems generating peer co-constructed 'interpersonal data' (Goulden, et al., 2018) and addressing collective harms of categorisation for groups (Taylor, et al., 2016).

The ePD applies to communications and tracking via IoT devices (Article 29 Data Protection Working Party, 2014) as will the ePR (Recital 12, ePR). Thus, machine to machine sharing of emotion data by devices, as required by appraisal-based methods, come within its scope. This is important, as the principle of confidentiality of communications applies (Art 5, ePD and ePR). In the ePD, this technical principle broadly prohibits any 'listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users' unless there is consent or lawful grounds to do so (Art 5(1) ePD). The latter might be where an EU member state has passed a law that is a necessary, appropriate and proportionate measure e.g., to safeguard

national security, law enforcement etc. (Art 15(1) ePD). Or similarly, terminal device storage or access is not prohibited when it is solely for transmitting a communication or for providing a service explicitly requested by the user (Art 5(3), ePD). With machine-to-machine processing, the service provision often, by design, relies on data flows below human intervention and oversight. Trust that infrastructure for enabling communications is confidential will be a key dimension here (Storms, 2018), and formulating that trust, as we discuss below, may rely on designing more contextually appropriate consent notifications in conjunction with more transparent information.

Type of network: How devices are networked remains a critical question for application of ePD, as it does not apply to private networks. The ePD applies to 'publicly available electronic communications networks' and 'services' (s32 and s151, UK Communications Act 2003). Broadly, the former means the infrastructure created to enable communications with electronic signals such as 3G networks and broadband networks. The service component focuses on giving the public access to this e.g., ISPs or mobile telco firms are service providers. With smaller, non-publicly available networks, it raises interesting questions about when it reaches the scale to be deemed publicly available. There is uncertainty about if industry led smart city network infrastructure, for example, would be deemed sufficiently public for ePD purposes (Edwards, 2018) although, ePR clarifies that it would apply to public WiFi networks and hotspots in semi-private and public places (Recital 13). It still would not apply to corporate networks only open to network members (Art 2(2)(c), ePR). Thus, local, home or even body area networks which may use different shorter range IoT communication protocols for EAI data sharing (e.g., heart rate data from wearables sharing by Bluetooth with phone) are unlikely to be considered within scope of the law (as closed networks are not publicly available). However, IoT devices often rely on cloud infrastructure to enable subsequent data analytics (which may see data sent over 3G or WiFi networks), hence they interact with public networks, and arguably are covered by Art 5(3) (Recital 56 ePD; Edwards, 2018). Developments in edge computing technologies, where data analysis occurs at the edge of the network on local devices may shift away from current cloud based IoT business models (Crabtree, et al., 2018, Singh, et al., 2018). As these scale, further analysis on to what extent public networks are used might be necessary to unpack the relationship with ePD (Urquhart, Lodge and Crabtree, 2019).

Sensing context: This is key for understanding the legality of collecting and linking together otherwise disparate data points to sense context. Computing context returns us to longstanding challenges of ubicomp sensing where 'when computation is moved "off the desktop," then we suddenly need to keep track of where it has gone' [24]. Risks around opacity of data flows, lack of user interfaces for consent and insecure devices enabling data breaches have plagued regulation of IoT (Brown, 2015), and could challenge EAI too. An emerging challenge for EAI in retail advertising could be real time bidding, where advertisers bid just in time for space to target adverts to consumers. The infrastructure of real time bidding involves significant data sharing between bidders and bidees, with little respect for data governance with the U.K. DP regulator, the ICO, stating "profiles created about individuals are extremely detailed and are repeatedly shared among hundreds of organisations for any one bid request, all without the individuals' knowledge." [25]. They also recognise that cross device tracking is a governance priority area particularly as information collected and shared as part of real time bidding infrastructure is vast, including location, time zone, device type, demographics, activity on site and search queries (U.K. Information Commissioner Office (ICO), 2019c).

They do not mention emotion data specifically, but risks of targeting with ads at precise moments of emotional frailty or vulnerability are clear, with appraisal-based methods providing contextual information to target those ads more effectively. As they collect a mixture of data regulated under both ePrivacy and GDPR (where it is personal) the interplay between these laws will be important.

ALthough EAI data may not always single out an individual, concerns about consent outlined above remain important, as ePD requires it, even if data stored or accessed on a device is not personal (Kosta, 2013; U.K. Information Commissioner Office (ICO), 2019b). For example, in addition to more conventional 'cookies', device identifiers and device fingerprinting approaches that can be used for online tracking are subject to the same consent requirements (A29 WP, 2014).

Considering the type of data that might be useful in appraisal-based approaches, location data is key. The ePR seeks to go further than ePD by prohibiting collection of 'information emitted from terminal equipment' when it tries to connect to another device or any network equipment. This could be particularly valuable for appraisal and context in EAI. Companies attempt to track device movements without using telco location data, by observing MAC, IMSI or IMEI addresses from phones or other devices seeking to conduct a handshake with a base station for authorisation and internet access. (Recital 20 & 25, ePR). This is particularly prized in retail, as firms have done this using WiFi enabled bins, to see how long shoppers stop and how many there are (Shubber, 2013). Some firms, like Apple, use a randomized MAC address in an attempt to avoid this, but this raises further security issues (Claburn, 2017). The law would permit such collection 'when it is exclusively to establish a connection (for the necessary amount of time)' or 'when a 'clear and prominent notice' is displayed with, at minimum the modalities of the collection, its purpose, person responsible for it' plus the various Art 13 GDPR information informational requirements discussed below (Recital 25 and Art 8(2) ePR). In particular, they would like prominent notices displayed about the geographic area (before the subject enters it), the purpose of processing, contact details of the processor and approaches to prevent and cease collection (Recital 25, ePR).

If we consider this alongside earlier discussions on audio-visual surveillance (and requirement there to display notices) it seems clear that use of such data in appraisal based systems needs to be sufficiently clear to data subjects, and their consent must be present. This is a push towards protection through user experience design, which clearly has much to offer here (Porter Felt, et al., 2016).

It is longstanding best practice for public space surveillance camera operators to display notices about areas being monitored (Art 29 WP, 2004). Art 12/13 GDPR will require further information on any notices by stating that the form and requirement for transparency of information around processing needs to be "concise, transparent, intelligible and easily accessible, using clear and plain language [especially for children]" (Art 12, GDPR). This includes the identity and contact details of controllers/DPOs, purpose of processing, legal basis for and where processing is based, legitimate interests that controllers are pursuing, recipients and categories of recipients for the personal data and any intended third country transfer (Art 13, GDPR). Use of (machine readable) icons is also

encouraged for Art 13 information delivery in ‘an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing.’ (Art 12(7), GDPR)

Clearly then, there is a greater need for notifications on devices and in public for transparency requirements, for collection of data emitted from devices or for consent (as collecting data for additional value added services or for accessing/storing information on terminal devices).

Public display and device notification design to explore the opportunities for creating legally compliant interfaces for EAI applications will require insights from design, technology and governance communities. Just in time notifications, vs. more static approaches, and also ensuring greater transparency and accountability around processing are not just ethically advisable, but legally required. These legal requirements create design opportunities, as opposed to constraints, and ways to formulate more trusting relationships between service providers and users, as we move into appraisal based public space EAI. As with browser cookies, use of tracking approaches which store or access information on devices of users require prior, informed ‘opt in’ consent (as opposed to it being opt out consent, which it was prior to the law change in 2009). As both ePD and the GDPR require consent for context-based EAI, and legitimate interests are increasingly being framed more narrowly, it makes sense to focus on understanding how to design for consent with public space EAI.

Considering the ‘trajectory’ of the user experience (UX) (Benford, et al., 2009) with a system could help in designing consent mechanisms, by examining the nature of the interface, the types of users, how long they interact with it and in what domain (Urquhart and Rodden, 2017). With multiple devices feeding the mosaic of emotional state detection, there are numerous UX possibilities where devices have varying affordances and signifiers to communicate consent information with users (Norman, 2014). Mobile devices are the most obvious interface for doing this, but what about other devices used in appraisal based approaches with different affordances for communicating with users? How could the overarching picture of processing be coordinated and communicated across devices and controllers, where their relationship may not be as formal as contractual joint controllers (Art 26, GDPR; Chen, et al., forthcoming) or processors/controllers (Ch IV, GDPR)? In some domains, there may be a contract between subject and controller (as terms and conditions could be used when someone enters a semi-public space like a music festival — as happened during the heavy metal festival, Download 2015 — where use of facial recognition was mentioned in tickets). But a ‘contractual nexus’ may not always exist in public space processing (Edwards, 2018) and this can complicate the legal process of mapping out legal obligations of different stakeholders (particularly around aggregation, access and sharing of information by EAI providers). There is a lot of literature in HCI about how to design for notifications (Fischer, et al., 2010; Luger and Rodden, 2013), and creating shared user experiences in public space (Flintham, et al., 2015). We believe there are opportunities for legally informed user centric interaction design to address and align interactional, design and governance questions posed by public space appraisal based EAI.

Conclusion

This paper has argued that we need to prepare for the emergence of appraisal-based emotional AI (EAI). It first briefly depicted the historical context of face-based EAI, highlighted weaknesses in "basic" approaches, and then argued that wide recognition of limitations with these methods will inevitably create interest in appraisal-based approaches. These will be more invasive due to need for extra data on internal (involving metabolic and experiential factors) and external contexts (such as when and where a person is, who they are with, perhaps even what they are saying, and by what means, e.g., in-person or through a device). Given the legal challenges in commercial use of such data, we see a need for ethical, normative and governance recognition that, despite private investment in cities and other urban spaces, applies public standards to private networks that are used in the course of their daily lives (such as shopping). In particular, we need to consider how to design EAI systems according to different deployment contexts, and associated legal requirements. In public spaces this can be difficult because the law is currently quite fragmented regarding EAI. Moreover, current and nascent infrastructures of EAI challenge fundamental concepts within the law.

As we pre-empt the shift to contextual, appraisal based approaches, it will more clearly involve personal data, and thus we can explore how DP law applies to the mosaic of information processing that enables emotional sorting. However, implementing and realising the content of those laws in practice requires support from the EAI design community. The public setting raises challenges around establishing responsible actors for data governance, how to design user interfaces and experiences for more ephemeral interactions, and to question if it is even ethical to deploy EAI in the first place (as we are seeing with debates around facial recognition). Yet, with EAI, the scope for perceived harm is significant; it enables systematic reading of emotional life whilst concurrently limiting scope for resistance, enables deeper reading for manipulation, all whilst using perceived intention as a mechanism for surveillance. As the legal framework remains focused on identification harms, it is often not best placed to deal with harms stemming from perceptions of subject intentionality (which EAI seeks). By anticipating EAI's turn to context, we can begin to better navigate the application and gaps of the currently fragmented governance, to ensure responsible innovation in this domain and better understanding of how best to protect subjects' rights. End of article

About the authors

Andrew McStay is Professor of Digital Life at Bangor University (Wales).

E-mail: mcstay@bangor.ac.uk

Lachlan Urquhart is Lecturer in Technology Law at the School of Law, University of Edinburgh and Visiting Researcher at the Horizon Digital Economy Research Institute, School of Computer Science, University of Nottingham.

E-mail: Lachlan.urquhart@.ed.ac.uk

Acknowledgements

We thank the ESRC for support through our grant: ES/S013008/1.

Notes

1. McDuff and Czerwinski, 2018, p. 79.

2. Ibid.

3. https://landsec.com/policies/privacy-policy/piccadilly-lights-english.

4. See https://www.sbxl.com/retail-the-secret-psychology/.

5. See https://docs.aws.amazon.com/rekognition/latest/dg/what-is.html.

6. See https://cloud.google.com/vision/docs/detecting-faces#vision_face_detection_gcs-go.

7. Marx, 2003, p. 200.

8. Verbeek, 2011, p. 9.

9. In EU parlance, a ‘Regulation’ is a legal instrument that applies in the same way in all member states (MS), without need for further MS legislation to instantiate the law. A Directive, in contrast, does require additional MS law, leading to subtle differences in each how each MS instantiates the law.

10. Carey, 2018, p. 13.

11. U.K. Information Commissioner Office (ICO), 2017, p. 6.

12. U.K. Information Commissioner Office (ICO), 2019a, p. 1.

13. Art 14, GDPR; EDPB, 2019a, paragraph 54.

14. EDPB, 2019a, paragraph 7.

15. EDPB, 2019a, paragraph 75.

16. EDPB, 2019a, paragraph 79.

17. Ibid.

18. EDPB, 2019a, pp. 9–11.

19. https://privacyblogfullservice.huntonwilliamsblogs.com/wp-content/uploads/sites/28/2019/07/edpb_guidelines_201903_videosurveillance.pdf.

20. EDPB, 2019a, paragraph 37.

21. EDPB, 2019b, paragraph 14.

22. EDPB, 2019b, paragraphs 40–41.

23. EDPB, 2019b, paragraphs 29–31; Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH, paragraphs 33–34.

24. Dourish, 2004, p. 20.

25. U.K. Information Commissioner Office (ICO), 2019c, p. 23.

References

Ada Lovelace Institute, 2019. “Beyond face value: Public attitudes to facial recognition technology” (2 September), at https://www.adalovelaceinstitute.org/beyond-face-value-public-attitudes-to-facial-recognition-technology/, accessed 23 September 2019.

F. Altenberger and C. Lenz, 2018. “A non-technical survey on deep convolutional neural network architectures,” arXiv (6 March), at https://arxiv.org/abs/1803.02129, accessed 23 September 2019.

Article 29 Data Protection Working Party, 2004. “Opinion 4/2004 on the processing of personal data by means of video surveillance” (11 February), at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp89_en.pdf, accessed 23 September 2019.

L.F. Barrett, R. Adolphs, S. Marsella, A.M. Martinez and S.D. Pollak, 2019. “Emotional expressions reconsidered: Challenges to inferring emotion from human facial movements,” Psychological Science in the Public Interest, volume 20, number 1, pp. 1–68.

doi: https://doi.org/10.1177/1529100619832930, accessed 23 September 2019.

S. Benford, G. Giannachi, B. Koleva and T. Rodden, 2009. “From interaction to trajectories: Designing coherent journeys through user experiences,” CHI ’09: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 709–718.

doi: https://doi.org/10.1145/1518701.1518812, accessed 23 September 2019.

I. Brown, 2015. “GSR discussion paper: Regulation and the Internet of things,” International Telecommunications Union (25 June), at https://www.itu.int/en/ITU-D/Conferences/GSR/Documents/GSR2015/Discussion_papers_and_Presentations/GSR_DiscussionPaper_IoT.pdf, accessed 23 September 2019.

P. Carey, 2018. Data protection: A practical guide to UK and EU law. Fifth edition. Oxford: Oxford University Press.

A. Cawsey, 1998. The essence of artificial intelligence. Harlow: Prentice Hall.

J. Chen, L. Edwards, L. Urquhart and D. McAuley, forthcoming. “Fair reassignment of responsibility and accountability in smart homes: Joint controllership and household exemption as legal mechanisms and their limitations.”

T. Claburn, 2017. “MAC randomization: A massive failure that leaves iPhones, Android mobes open to tracking,” Register (10 March), at https://www.theregister.co.uk/2017/03/10/mac_address_randomization/, accessed 23 September 2019.

D. Clifford, 2017. “Citizen-consumers in a personalised galaxy: Emotion influenced decision-making, a true path to the dark side?” CiTiP Working Paper Series, at https://ssrn.com/abstract=3037425, accessed 23 September 2019.

doi: http://dx.doi.org/10.2139/ssrn.3037425, accessed 23 September 2019.

Council of the European Union, 2018. “Progress report on the proposal for a Regulation on Privacy and Electronic Communications” (23 November), at http://data.consilium.europa.eu/doc/document/ST-14491-2018-INIT/en/pdf, accessed 23 September 2019.

A. Crabtree, T. Lodge, J. Colley, C. Greenhalgh, K. Glover, H. Haddadi, Y. Amar, R. Mortier, Q. Li, J. Moore, L. Wang, Y. Poonam, J. Zhao, A. Brown, L. Urquhart and D. McAuley, 2018. “Building accountability into the Internet of things: The IoT databox model,” Journal of Reliable Intelligent Environments, volume 4, number 1, pp. 39–55.

doi: https://doi.org/10.1007/s40860-018-0054-5, accessed 23 September 2019.

K. Crawford, 2019. “Halt the use of facial-recognition technology until it is regulated,” Nature, volume 572, number 7771 (27 August), p. 565, at https://www.nature.com/articles/d41586-019-02514-7, accessed 23 September 2019.

doi: https://doi.org/10.1038/d41586-019-02514-7, accessed 23 September 2019.

C. Darwin, 2009. The expression of the emotions in man and animals. Oxford: Oxford University Press.

B. Davies, M. Innes and A. Dawson, 2018. “An evaluation of South Wales use of facial recognition,” Cardiff: Universities’ Police Science Institute, Crime & Security Research Institute, Cardiff University, at https://crimeandsecurity.org/feed/afr, accessed 23 September 2019.

G. Deleuze, 1992. “Postscript on the societies of control,” October, volume 59, pp. 3–7.

M. Dodge and R. Kitchin, 2007. “‘Outlines of a world coming into existence’: Pervasive computing and the ethics of forgetting,” Environment and Planning B: Urban Analytics and City Science, volume 34, number 3, pp. 431–445.

doi: https://doi.org/10.1068/b32041t, accessed 23 September 2019.

P. Dourish, 2004. “What talk about when we talk about context,” Personal and Ubiquitous Computing, volume 8, number 1, pp. 19–30.

doi: https://doi.org/10.1007/s00779-003-0253-8, accessed 23 September 2019.

G.–B. Duchenne, 1990. The mechanism of human facial expression. Edited and translated by R.A. Cuthbertson. Cambridge: Cambridge University Press.

L. Edwards, 2018. “Data protection and e-privacy: From spam and cookies to big data, machine learning and profiling,” In: L. Edwards (editor). Law, policy and the Internet. Oxford: Hart Publishing.

L. Edwards, 2016. “Privacy, security and data protection in smart cities: A critical EU law perspective,” European Data Protection Law Review, volume 2, number 1, pp. 28–58.

doi: https://doi.org/10.21552/EDPL/2016/1/6, accessed 23 September 2019.

L. Edwards, 2004. “Taking the ‘personal’ out of personal data: Durant v FSA and its impact on the legal regulation of CCTV,” SCRIPT-ed, volume 1, number 2, pp. 341–349, and at https://script-ed.org/wp-content/uploads/2016/07/1-2-Edwards.pdf, accessed 23 September 2019.

P. Ekman and W.V. Friesen, 1978. Facial action coding system: Investigator’s guide. Palo Alto, Calif.: Consulting Psychologists Press.

P. Ekman and W.V. Friesen, 1971. “Constants across cultures in the face and emotion,” Journal of Personality and Social Psychology, volume 17, number 2, pp. 124–129.

doi: http://dx.doi.org/10.1037/h0030377, accessed 23 September 2019.

ePrivacy Directive (ePD), 2002. “ePrivacy Directive 2002/58/EC as amended by DIRECTIVE 2009/136/EC,” at https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002L0058:20091219:EN:PDF, accessed 23 September 2019.

ePrivacy Regulation (ePR), 2017. “Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) Brussels, 10.1.2017 COM (2017) 10 final 2017/0003 (COD),” at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010, accessed 23 September 2019.

EU Parliament, 2019. “Legislative train schedule, connected digital single market,” at https://www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market/file-jd-e-privacy-reform, accessed 23 September 2019.

European Data Protection Board (EDPB), 2019a. “Guidelines 3/2019 on processing of personal data through video devices” (10 July), at https://edpb.europa.eu/our-work-tools/public-consultations/2019/guidelines-32019-processing-personal-data-through-video_en, accessed 23 September 2019.

European Data Protection Board (EDPB), 2019b. “Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities” (12 March), at https://edpb.europa.eu/sites/edpb/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf, accessed 23 September 2019.

L. Fernandez and L. Huey, 2009. “Is resistance futile? Thoughts on resisting surveillance,” Surveillance and Society, volume 6, number 3, at https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/3280, accessed 23 September 2019.

doi: https://doi.org/10.24908/ss.v6i3.3280, accessed 23 September 2019.

J.E. Fischer, N. Yee, V. Bellotti, N. Good, S. Benford and C. Greenhalgh, 2010. “Effects of content and time of delivery on receptivity to mobile interruptions,” MobileHCI ’10: Proceedings of the 12th International Conference on Human Computer Interaction with Mobile Devices and Services, pp. 103–112.

doi: https://doi.org/10.1145/1851600.1851620, accessed 23 September 2019.

M.D. Flintham, R. Velt, M.L. Wilson, E.J. Anstead, S. Benford, A. Brown, T. Pearce, D. Price and J. Sprinks, 2015. “Run spot run: Capturing and tagging footage of race by crowds of spectators,” CHI ’15: Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, pp. 747–756.

doi: https://doi.org/10.1145/2702123.2702463, accessed 23 September 2019.

B.J. Fogg, 2002. “Persuasive technology: Using computers to change what we think and do,” Ubiquity, volume 2002, article number 5.

doi: http://dx.doi.org/10.1145/764008.763957, accessed 23 September 2019.

Forbrukerrådet, 2018. “Deceived by design: How tech companies use dark patterns to discourage us from exercising our rights to privacy” (27 June), at https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf, accessed 23 September 2019.

Gartner, 2018. “Emotion AI will personalize interactions” (22 January), at https://www.gartner.com/smarterwithgartner/emotion-ai-will-personalize-interactions, accessed 23 September 2019.

General Data Protection Regulation (GDPR), 2016. “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC,” at https://publications.europa.eu/en/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1/language-en, accessed 22 September 2019.

M. Goulden, P. Tolmie, R. Mortier, T. Lodge, A.–K. Pietilainen and R. Teixeira, 2018. “Living with interpersonal data: Observability and accountability in the age of pervasive ICT,” New Media & Society, volume 20, number 4, pp. 1,580–1,599.

doi: https://doi.org/10.1177/1461444817700154, accessed 23 September 2019.

S. Graham, 2009. “Cities as battlespace: The new military urbanism,” City, volume 13, number 4, pp. 383–402.

doi: http://dx.doi.org/10.1080/13604810903298425, accessed 23 September 2019.

A. Greenfield, 2013. Against the smart city. New York: Do Projects.

J. Grudin, 1990. “The computer reaches out:The historical continuity of interface design,” CHI ’90: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 261–268.

doi: https://doi.org/10.1145/97243.97284, accessed 23 September 2019.

H. Gunes and M. Pantic, 2010. “Automatic, dimensional and continuous emotion recognition,” International Journal of Synthetic Emotions, volume 1, number 1, pp. 68–99.

doi: http://dx.doi.org/10.4018/jse.2010101605, accessed 23 September 2019.

K.D. Haggerty and R.V. Ericson, 2000. “The surveillant assemblage,” British Journal of Sociology, volume 51, number 4, pp. 605–622.

doi: http://dx.doi.org/10.1080/00071310020015280, accessed 23 September 2019.

R. Kitchin, 2014. “The real-time city? Big data and smart urbanism,” GeoJournal, volume 79, number 1, pp. 1–14.

doi: https://doi.org/10.1007/s10708-013-9516-8, accessed 23 September 2019.

E. Kosta, 2013. “Peeking into the cookie jar: the European approach towards the regulation of cookies,” International Journal of Law and Information Technology, volume 21, number 4, pp. 380–406.

doi: https://doi.org/10.1093/ijlit/eat011, accessed 23 September 2019.

Law Society, 2019. “Algorithms in the criminal justice system report” (4 June), at https://www.lawsociety.org.uk/support-services/research-trends/algorithm-use-in-the-criminal-justice-system-report/, accessed 23 September 2019.

Z.C. Lipton, J. Berkowitz and C. Elkan, 2015. “A critical review of recurrent neural networks for sequence learning,” arXiv (29 May), at https://arxiv.org/abs/1506.00019, accessed 23 September 2019.

E. Luger and T. Rodden, 2013. “An informed view on consent for UbiComp,” UbiComp ’13: Proceedings of the 2013 ACM International Joint Conference on Pervasive and Ubiquitous Computing, pp. 529–538.

doi: https://doi.org/10.1145/2493432.2493446, accessed 23 September 2019.

D. Lyon (editor), 2003. Surveillance as social sorting: Privacy, risk, and digital discrimination. New York: Routledge.

B. Martinez, M.F. Valstar, B. Jiang and M. Pantic, 2017. “Automatic analysis of facial actions: A survey,” IEEE Transactions on Affective Computing, volume 10, number 3, pp. 325–347.

doi: https://doi.org/10.1109/TAFFC.2017.2731763, accessed 23 September 2019.

G.T. Marx, 2003. “A tack in the shoe: Neutralizing and resisting the new surveillance,” Journal of Social Issues, volume 59, number 2, pp. 369390.

doi: https://doi.org/10.1111/1540-4560.00069, accessed 23 September 2019.

V. Mayer-Schönberger, 2009. Delete: The virtue of forgetting in the digital age. Princeton, N.J.: Princeton University Press.

D. McDuff and M. Czerwinski, 2018. “Designing emotionally sentient agents,” Communications of the ACM, volume 61, number 12, pp. 74–83.

doi: http://dx.doi.org/10.1145/3186591, accessed 23 September 2019.

D. McDuff and R. el Kaliouby, 2017. “Applications of automated facial coding in media measurement,” IEEE Transactions on Affective Computing, volume 8, number 2, pp. 148–160.

doi: http://dx.doi.org/10.1109/TAFFC.2016.2571284, accessed 23 September 2019.

A. McStay, 2018. Emotional AI: The rise of empathic media. London: Sage.

A. McStay, 2017. “An ethical intervention into conscious cities,” Conscious Cities Journal, number 3, at https://theccd.org/articles/ethical-intervention-conscious-cities, accessed 23 September 2019.

A. McStay, 2016. “Empathic media and advertising: Industry, policy, legal and citizen perspectives (the case for intimacy),” Big Data & Society, (23 November).

doi: https://doi.org/10.1177/2053951716666868, accessed 23 September 2019.

A. McStay, 2014. Privacy and philosophy: New media and affective protocol. New York: Peter Lang.

A. McStay, V. Bakir, P. Mantello and L. Urquhart, 2019. “Cross cultural conversations between Japan and UK on emotional AI,” Report of ESRC Project ES/S013008/1, at https://emotionalai.org/projects, accessed 23 September 2019.

T. Monahan, 2015. “The right to hide? Anti-surveillance camouflage and the aestheticization of resistance,” Communication and Critical/Cultural Studies, volume 12, number 2, pp. 159–178.

doi: http://dx.doi.org/10.1080/14791420.2015.1006646, accessed 23 September 2019.

H. Nissenbaum, 2010. Privacy in context: Technology, policy, and the integrity of social life. Stanford, Calif.: Stanford Law Books.

D.A. Norman, 2014. The design of everyday things. Revised and expanded edition. Cambridge, Mass.: MIT Press.

A. Porter Felt, R.W. Reeder, A. Ainslie, H. Harris, M. Walker, C. Thompson, M.E. Acer, E. Morant and S. Consolvo, 2016. “Rethinking connection security indicators,” SOUPS ’16: Proceedings of the Twelfth USENIX Conference on Usable Privacy and Security, pp. 1–13, and at https://www.usenix.org/system/files/conference/soups2016/soups2016-paper-porter-felt.pdf, accessed 23 September 2019.

M. Quigley and S. Ayihongbe, 2018. “Everyday cyborgs: On integrated persons and integrated goods,” Medical Law Review, volume 26, number 2, pp. 276–308.

doi: https://doi.org/10.1093/medlaw/fwy003, accessed 23 September 2019.

S. Ren, K. He, R. Girshick and J. Sun, 2015. “Faster R-CNN: Towards real-time object detection with region proposal networks,” arXiv (4 June), at https://arxiv.org/abs/1506.01497, accessed 23 September 2019.

J.A. Russell, 1994. “Is there universal recognition of emotion from facial expression? A review of the cross-cultural studies,” Psychological Bulletin, volume 115, number 1, pp. 102–141.

doi: http://dx.doi.org/10.1037/0033-2909.115.1.102, accessed 23 September 2019.

Sensing Feeling, 2018. “Advanced human emotion sensing products for business,” at https://sensingfeeling.io/#, accessed 23 September 2019.

M. Shepard, 2011. “Introduction,” In: M. Shepard (editor). Sentient city: Ubiquitous computing, architecture, and the future of urban space. Cambridge, Mass.: MIT Press.

K. Shubber, 2013. “Tracking devices hidden in London’s recycling bins are stalking your smartphone,” Wired (9 August), at https://www.wired.co.uk/article/recycling-bins-are-watching-you, accessed 23 September 2019.

J. Singh, T. Pasquier, J. Bacon, J. Powles, R. Diaconu and D. Eyers, 2016. “Big ideas paper: Policy-driven middleware for a legally-compliant Internet of things,” Middleware ’16: Proceedings of the 17th International Middleware Conference, article number 13.

doi: https://doi.org/10.1145/2988336.2988349, accessed 23 September 2019.

D.J. Solove, 2006. “A taxonomy of privacy,” University of Pennsylvania Law Review, volume 154, number 3, pp. 477–564.

doi: https://doi.org/10.2307/40041279, accessed 23 September 2019.

S. Song, L. Shen and M. Valstar, 2018. “Human behaviour-based automatic depression analysis using hand-crafted statistics and deep learned spectral features,” 2018 13th IEEE International Conference on Automatic Face & Gesture Recognition (FG 2018), pp. 158–165.

doi: https://doi.org/10.1109/FG.2018.00032, accessed 23 September 2019.

E.R. Sorenson, 1976. The edge of the forest: Land, childhood and change in a New Guinea protoagricultural society. Washington, D.C.: Smithsonian Institution Press.

S. Storms, 2018. “Quo vadis, ePrivacy? Confidentiality of machine-to-machine communications,” Centre for IT & IP Law (Katholieke Universiteit Leuven, [KU Leuven]) blog (26 June), at https://www.law.kuleuven.be/citip/blog/quo-vadis-eprivacy-confidentiality-of-machine-to-machine-communications/, accessed 23 September 2019.

L. Taylor, L. Floridi and B. van der Sloot (editors), 2017. Group privacy: New challenges of data technologies. Cham, Switzerland: Springer International.

doi: https://doi.org/10.1007/978-3-319-46608-8, accessed 23 September 2019.

G. Topham, 2018. “The end of road rage? A car which detects emotion,” Guardian (23 January), at https://www.theguardian.com/business/2018/jan/23/a-car-which-detects-emotions-how-driving-one-made-us-feel, accessed 23 September 2019.

J. Turow, 2017. The aisles have eyes: How retailers track your shopping, strip your privacy, and define your power. New Haven, Conn.: Yale University Press.

U.K. Information Commissioner Office, 2019a. “Live facial recognition technology — Data protection law applies,” ICO Blog, at https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/blog-live-facial-recognition-technology-data-protection-law-applies/, accessed 23 September 2019.

U.K. Information Commissioner Office, 2019b. “Guidance on use of cookies and similar technologies” (3 July), at https://ico.org.uk/media/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies-1-0.pdf, accessed 23 September 2019.

U.K. Information Commissioner Office (ICO), 2019c. “Update report into adtech and real time bidding” (20 June), at https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf, accessed 23 September 2019.

U.K. Information Commissioner Office (ICO), 2017. “In the picture: A data protection code of practice for surveillance cameras and personal information,” at https://ico.org.uk/media/1542/cctv-code-of-practice.pdf, accessed 23 September 2019.

L. Urquhart and T. Rodden, 2017. “New directions in information technology law: Learning from human-computer interaction,” International Review of Law, Computers & Technology, volume 31, number 2, pp. 150–169.

doi: https://doi.org/10.1080/13600869.2017.1298501, accessed 23 September 2019.

L. Urquhart, H. Schnädelbach and N. Jäger, 2019. “Adaptive architecture: Regulating human building interaction,” International Review of Law, Computers & Technology, volume 33, number 1, pp. 3–33.

doi: https://doi.org/10.1080/13600869.2019.1562605, accessed 23 September 2019.

L. Urquhart, T. Lodge and A. Crabtree, 2019. “Demonstrably doing accountability for the Internet of Things,” International Journal of Law and Information Technology, volume 27, number 1, pp. 1–27.

doi: https://doi.org/10.1093/ijlit/eay015, accessed 23 September 2019.

L. Urquhart, N. Sailaja and D. McAuley, 2018. “Realising the right to data portability for the domestic Internet of Things,” Personal and Ubiquitous Computing, volume 22, number 2, pp. 317–332.

doi: https://doi.org/10.1007/s00779-017-1069-2, accessed 23 September 2019.

P.–P. Verbeek, 2011. Moralizing technology: Understanding and designing the morality of things. Chicago: University of Chicago Press.

P. Wiles, 2019. Annual report 2018: Commissioner for the retention and use of biometric material. London: Office of the Biometrics Commissioner, at https://www.gov.uk/government/publications/biometrics-commissioner-annual-report-2018, accessed 23 September 2019.

X. Wu and X. Zhang, 2017. "Responses to critiques on machine learning of criminality perceptions (Addendum of arXiv:1611.04135)," arXiv (26 May), at https://arxiv.org/abs/1611.04135, accessed 23 September 2019.

Case law

R [Bridges] v Chief Constable of South Wales Police and Secretary of State for the Home Department [2019], at https://www.judiciary.uk/wp-content/uploads/2019/09/bridges-swp-judgment-Final03-09-19-1.pdf, accessed 23 September 2019.

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH [2018], paragraphs 33–34, at http://curia.europa.eu/juris/liste.jsf?num=C-210/16, accessed 23 September 2019.

Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González [2014], at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131, accessed 23 September 2019.

Edem v Information Commissioner [2014], at https://uk.practicallaw.thomsonreuters.com/D-024-4261?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1, accessed 23 September 2019.

Durant v Financial Services Authority [2003], at https://www.ucpi.org.uk/wp-content/uploads/2019/03/Durant-v_FSA_2003_EWCA_Civ_1746.pdf, accessed 23 September 2019.