Government Office for Science

Foresight

Future Identities: Changing identities in the UK – the next 10 years

DR 5: How will surveillance and privacy technologies impact on the psychological notions of identity?

Ian Brown

Oxford Internet Institute, University of Oxford

January 2013

This review has been commissioned as part of the UK Government's Foresight project, *Future Identities: Changing identities in the UK – the next 10 years* . The views expressed do not represent policy of any government or organisation.

Contents

1. The likely direction of surveillance and privacy technologies[1]

Surveillance technologies gather, process, record, search and distribute information about individuals and their activities, sometimes partially at the instigation of the individual concerned. Privacy technologies restore some level of control over this data to the individual, reducing the ability of third parties to monitor their characteristics and activities without their explicit consent.

There are two key trends in the development of surveillance and privacy technologies over the next decade:

1. Surveillance will increasingly be deployed for pre-emptive purposes by governments and companies. This is driven by an increase in computing capacity, miniaturisation of devices and improvements in performance, together with increased public use of digital media.

2. Without a stronger impetus from regulators, the limited economic viability of privacy-protective technologies to date and reliance on ineffective privacy solutions means that privacy protection is lagging behind the development of surveillance technologies.

1.1 Cheaper, faster, more powerful surveillance capabilities

Modern Britain is filled with sensors such as CCTV cameras and mobile phones, with biometric and electronic identifiers increasingly used to link audio-visual, location and other types of data to individuals. Cheshire Constabulary estimated in 2011 that there are 1.85m CCTV cameras in the UK, 1.7m of which are privately owned – despite very limited evidence of their impact on crime levels (Gill and Spriggs 2005).

The combination of roadside cameras and automatic number plate recognition demonstrates the broad purposes to which surveillance systems can now be directed: “repressive surveillance (traffic offences), detective surveillance (stolen vehicles), the regulation of traffic flow (reduction of congestions), support for planning (recording information on all aspects of traffic), accident prevention (transmission of information to drivers on obstacles to anticipate) or the improvement of access times for emergency services (breakdowns, accidents)” (Lianos 2003: 415).

CCTV infrastructure is concentrated in urban areas. However, UK police forces are testing small aerial surveillance drones that can roam freely. These are likely to become cheaper, more reliable and much more widely used over the next ten years.

Very low-cost remotely readable RFID tags are increasingly attached to consumer goods and access control cards, the first wave of the “Internet of Things” that could make some aspects of the physical world as trackable as Internet activity. More sophisticated tags are included in many nations’ passports, and are also being used for road toll payment systems, public transport ticketing such as London’s Oyster card, and in new contactless payment cards such as MasterCard’s *PayPass* and Visa’s *Paywave*. In the next decade we are likely to see these

[1] This section is partially based on a 2010 report by the author for the European Commission on “The challenges to European data protection laws and principles”, which contains extensive references

sensors and tags become ubiquitous, dramatically smaller and much more capable through the application of nanotechnology.

Biometric measurements of biological or behavioural characteristics can be used to verify an individual's identity and to identify individuals or samples within population-scale databases such as the UK National DNA Database and National Fingerprint Database. Facial recognition software has been used to match photographs and video footage of individuals against databases of criminal suspects, so far with limited success – but is likely to improve significantly in performance over the next decade.

Health surveillance will increase with the increasing digitisation of patient records and widespread use of health sensors. The sequencing of patient genomes is likely to become routine, allowing individuals to check their susceptibility to diseases with genetic factors; clinicians to prescribe medication and other interventions tailored to patients; and insurers potentially to refuse coverage to the genetically disadvantaged.

1.2 Greater capacity and demand for data analysis

Underlying developments in computing technology will enable sophisticated analysis of this flood of personal data. Computer processing power is expected to continue following Moore's Law, doubling every 18-24 months – at least thirty-fold in the next decade, although by that point the fundamental limits of silicon engineering will be approaching. Computer storage capacity and communications bandwidth will likely continue increasing at least as quickly. These exponential increases will significantly enhance the capability of organisations to collect, store and process personal data – for law enforcement surveillance, for more efficient and personalised services, and for private-sector profiling for marketing, price discrimination and other purposes.

In response to security fears, rich-world governments are analysing and exchanging ever-greater quantities of information on their citizens, using data mining tools to identify individuals "of interest". In the near future, it will be so easy to put everyone under digital surveillance that it could easily become the default position. This includes international cooperation between public authorities aimed at identifying suspected football hooligans, illegal or trafficked migrants, political activists, terrorists and paedophiles. Being given any of these labels by any authority, in any country, can quickly lead to such a stigma becoming all-pervasive, without it being possible to challenge the body that initially made the mark.

Looking at a ten-year horizon, science fiction notions of "pre-crime" detection will become decreasingly fanciful. Research is already underway into detecting planned terrorist actions from brainwaves, pre-birth identification of future criminals based on parental and environmental conditions, and intelligent "thinking cameras" that can autonomously select targets for surveillance.

1.3 Greater sharing of data through digital media

The use of digital technologies in itself tends to generate records of personal activity in a form that can easily be stored, searched, shared and repurposed.

In the online environment almost every communication and Web page access leaves behind detailed footprints, linked to individuals through the IP address of their computer or

smartphone, and through digital “cookies” left on their browser by Web sites. Behavioural advertising companies track individuals across sites to show adverts targeted to their profiles; WPP already has built such profiles on 500m individuals in North America, Europe and Australia. European privacy regulators are making strenuous efforts to require explicit user consent for profiling. Mobile phones send location information to network providers to enable location-based services such as contextual advertising and mapping. All EU member states require telephone companies and Internet Service Providers to store data about their customers’ communications and location, for later police access.

Social media encourage individuals to share information about themselves with their “friends”, along with the operators of those sites and government agencies with legal powers to access this data. The 2011 Oxford Internet Survey found that 60% of UK Internet users use social networking sites to share a broad range of information about themselves and their family, friends and colleagues; this percentage is likely to increase as the most enthusiastic user population (students) ages (see fig. 1).

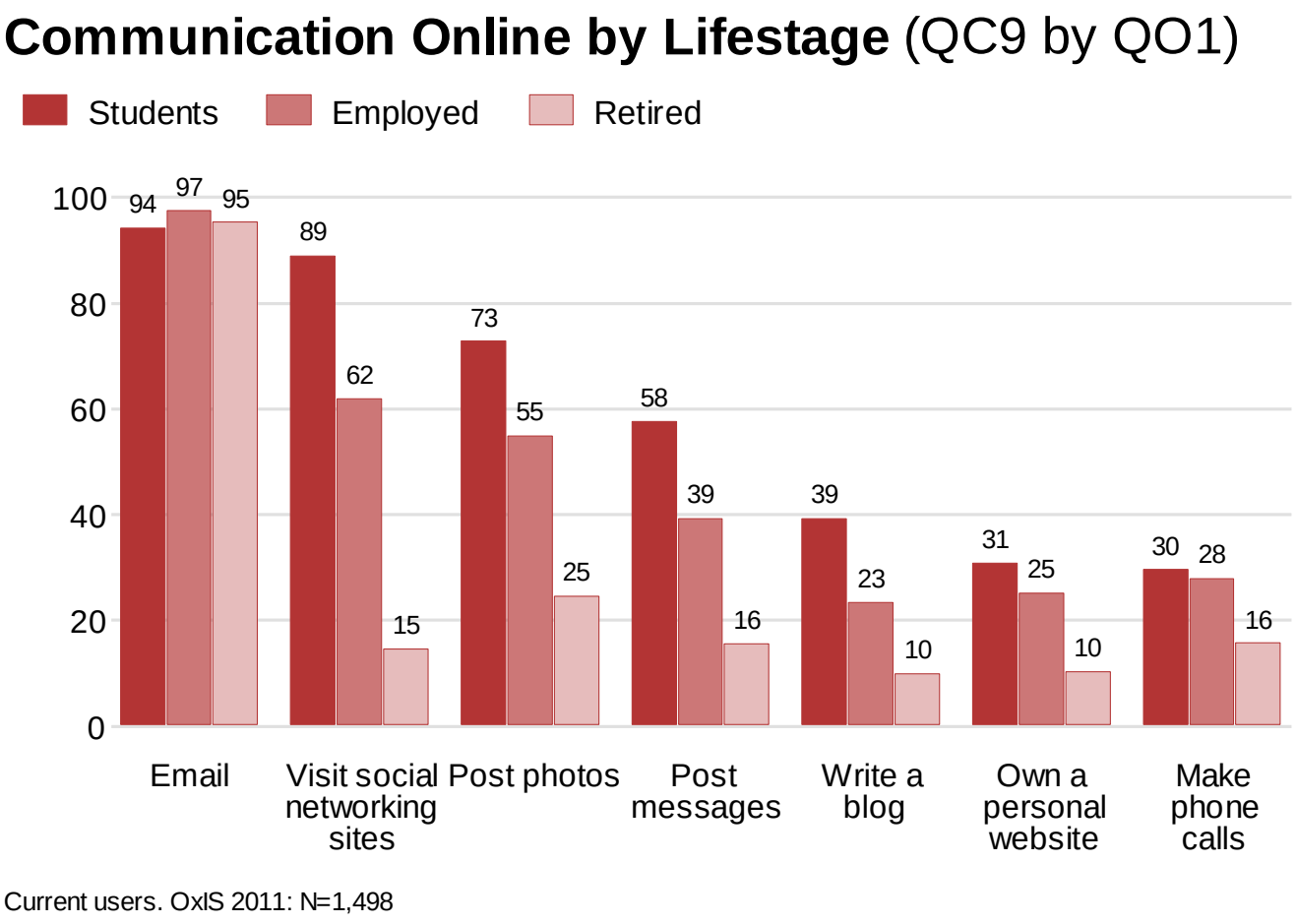
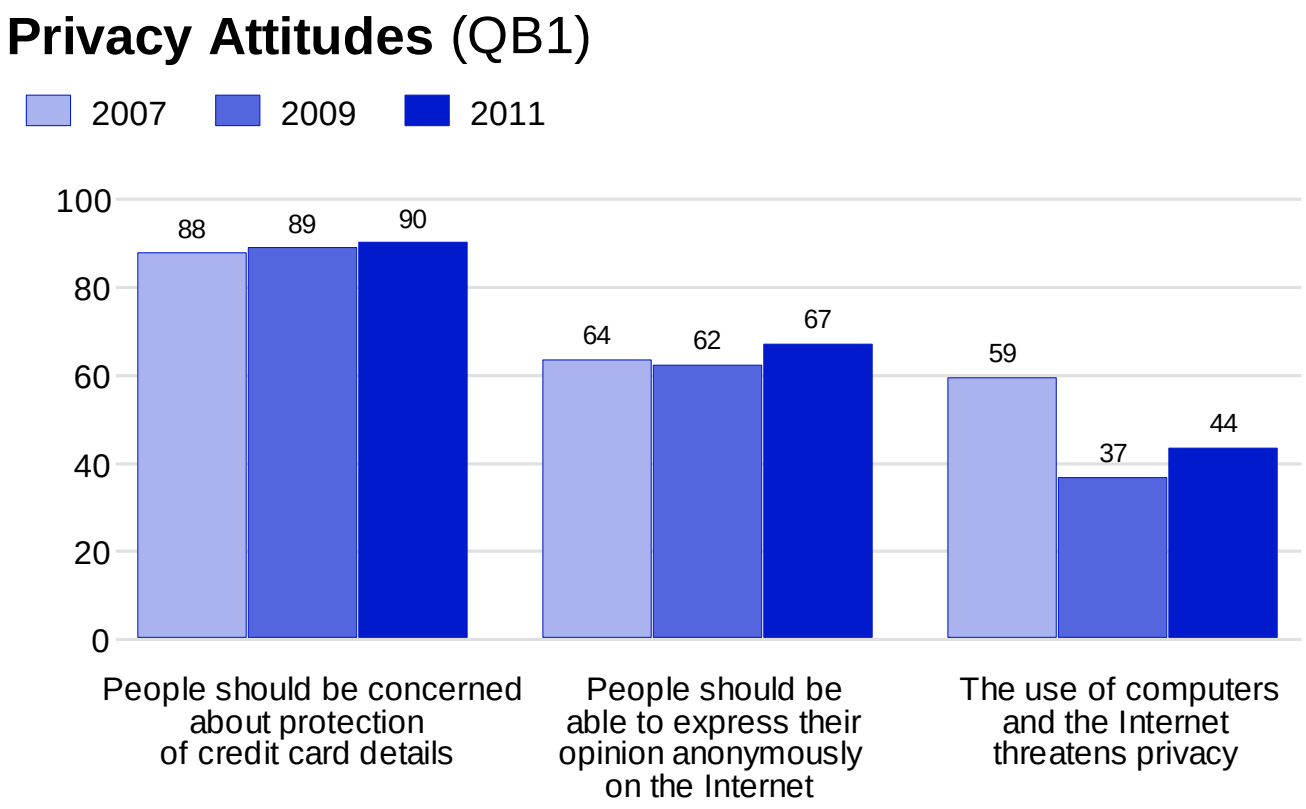


Figure 1: Communication Online by Lifestage. Source: Oxford Internet Survey 2011, Oxford Internet Institute

Gadgets such as heart rate monitors already allow individuals to share information about themselves and their environment through social media. This will become a pervasive phenomenon, with some individuals recording detailed information about every aspect of their lives (Askoxylakis *et al*. 2011). Privacy-sensitive individuals will have a limited ability to opt-out of such environmental sensing by others.

1.4 Continued development but limited use of privacy tools

Individuals continue to report concern about privacy, with a 2008 European Commission Flash Eurobarometer survey finding 38% of UK respondents “very concerned” and 39% “fairly concerned” whether their personal information is being protected by organisations. The 2011 Oxford Internet Survey found that 67% of respondents agreed “people should be able to express their opinion anonymously on the Internet”, while 44% were concerned that “the use of computers and the Internet threatens privacy” (see fig. 2).



OxIS 2007: N=2,350; OxIS 2009: N=2,013; OxIS 2011: N=2,057

Figure 2: Privacy Attitudes. Source: Oxford Internet Survey 2011, Oxford Internet Institute

Social networking sites such as Facebook provide detailed options for controlling who gets access to individual profiles and shared content – although researchers have found that these controls are often difficult to use and not prominent. Users rarely alter default settings, which therefore have a strong impact. The providers’ economic interests are generally in encouraging greater disclosure, while providing some less-prominent options for the quarter of the population identified by Westin (1999) as “privacy fundamentalists”.

Well-developed Internet communication tools and privacy-friendly identity management systems (such as Tor and Microsoft’s now-abandoned CardSpace) use encryption to prevent surveillance of online user activities. Digital payment services that mimic the anonymous nature of physical money are now several decades old. It would be possible for “cloud” services (such as Google Docs) to store and even process data only in encrypted form, or on users’ own computing equipment, ensuring that access is limited to the owners of that data.

However, the economics has so far been unfavourable for the deployment of all these “privacy enhancing technologies” (PETs), and is likely to remain so without regulatory intervention. Businesses see little government or consumer drive for PET deployment, and are reluctant to bear their costs without concrete evidence of benefits. Many Internet companies’ business models rely on “monetisation” of user data. Even so, a microeconomic analysis by Bohme and Koble (2007) showed that in most situations, businesses could increase revenues by allowing privacy-sensitive customers to use PETs in a transaction.

A 2010 London Economics study for the European Commission suggested that governments have an important role in setting privacy standards, supporting PET development and themselves upholding good practice. Encouragement of systems built to include “privacy by design” is one of the main purposes of the forthcoming EU Data Protection Regulation, but it is hard to predict how effective these measures will be. Their precursors in the current Data Protection Directive have had little impact.

2. Enabling and constraining impacts of these technologies on identity

A distinction is often drawn between an individual's identity – their defining attributes – and the representation and matching of such attributes, or 'identification' (Hildebrandt, 2008).

The most fundamental impact surveillance has on identity is that it reduces individuals' control over the information they disclose about their attributes in different social contexts, often to powerful actors such as the state or multinational corporations. Social networking sites are also making it much easier for information to be shared about individuals by their friends and acquaintances, with or without their permission. Any of these actors in turn may treat individuals differently based on that information, and share it without their explicit consent – including using identification technologies to link surveillance data back to individuals. Better and more widely available privacy technologies would give some of that control back to users.

Social interactionist theories of identity state that the self is reflected back from others (Cooley 1902) and wider society's cultural norms and standards (Mead, 1932). Individuals present different aspects of the self to different friends, family members, colleagues and strangers (Goffman 1959) and manage their relationships with others through selective disclosure of identity (Adams and Sasse 2001). Internet users spend a great deal of time curating online "exhibitions" of different aspects of their identities (Hogan 2010). People are "perceived quite differently in different domains" (McKenna 2007). As William James wrote in 1892: "A man has as many social selves as there are individuals who recognize him."

A reduction in disclosure control affects the ability of people to regulate effectively their social interactions (Joinson and Paine 2007) and position themselves in relation to available social identities. This violates the "contextual integrity" that individuals rely on to play different roles (worker, best friend, social club member, parent, child) in different social situations (Nissenbaum 2010). It also facilitates economic and governance aims, classifying and controlling individuals in more or less subtle ways, such as by using "risk profiles" to allocate credit or make decisions on individual passage through a border (Lianos 2003).

Individuals may feel that such classifications are blunt or miss important data relevant to the making of a fair decision. They may also have a "chilling effect" on the possibilities for whistleblowing and democratic activism, as demonstrated in the Information Commissioner's Office investigation into files covertly gathered on 3,200 "leftwing or troublesome" builders to block their further employment[2].

Technology-mediated activities' accessibility to surveillance, not present in face-to-face interactions, can make identity management more difficult. Information shared electronically is usually persistent (saved by default, perhaps indefinitely), searchable (much easier to find), replicable (easily shareable in convincing form), and as a result lacks a specific audience (Boyd 2008: 126). None of these qualities is obvious to less experienced users. Real-world gossip is deniable, usually geographically limited and fades over time. Digital information about an

[2] See http://www.guardian.co.uk/technology/2012/mar/03/police-blacklist-link-construction-workers. Accessed 12 December 2012

individual – however partial and unrepresentative – can persist as what Daniel Solove calls a "digital scarlet letter."

Identity play and control is especially important to young people as they grow up and develop their own independent identities and peer relationships. The use of social networks is now a key part of this process in advanced economies, critical for friendships, social capital and popularity (Joinson and Paine 2007; Livingstone 2006) and experimentation with different roles and types of identities (Moinian 2006).

Children can use private online spaces for "silly, rude or naughty behaviour" and to seek confidential information and advice (Livingstone 2006: 132). This can be vital for children that may feel isolated in their local environment, such as lesbian or gay teenagers, who can make friends online with geographically remote individuals (Marwick, Diaz and Palfrey 2010). But this "identity work" in social networks has a consequence usually unintended by the user: the development of commercial profiles that can have a significant impact on life chances.

Individuals' close social circle members can respond quite negatively to expressed identities that are contrary to an expected social role. The Internet has given individuals greater opportunities to express and develop marginalised identities (e.g. sexuality and fringe ideologies), and to overcome social anxiety. Active participation in online discussion groups related to stigmatised identities and ideologies allows individuals to gain support from group members, leading to increased self-acceptance and reduced feelings of isolation, difference and shame as well as significant increased willingness to ultimately share these identities with family and friends (McKenna 2007).

2.1 State surveillance

Law enforcement and intelligence agencies are extremely enthusiastic about accessing the "digital tsunami" of data about individuals being produced by modern surveillance technologies – both state-operated, and by access to private-sector data. Pre-emption rather than after-the-fact investigation is an emphasis in all of these schemes.

The UK's National Policing Improvement Agency operates a national DNA database, which is one of the world's largest, with profiles on an estimated 5,570,284 individuals as of 31 March 2012. It also operates a national automatic number plate recognition system, which by March 2011 was receiving 15 million sightings daily, with over 11 billion vehicle sightings stored. A national fingerprint database contained 8.3m individual's prints in April 2010. Government surveillance agency GCHQ has reportedly spent several hundred million pounds expanding its capabilities to intercept online communications in a "Mastering the Internet" programme, with claims of a total budget of over £1bn ($1.5bn) to give analysts complete visibility of UK Internet traffic (Brown 2012). Routine police "Forward Intelligence Team" surveillance of demonstrations and protestors has become common, although it has been challenged by a 2009 Court of Appeal judgment that retention of photographs must be justified on a case-by-case basis.

Law enforcement and intelligence agencies are also increasingly accessing and being supplied with data by the private sector, making surveillance processes more complex and likely to impact on these organizations' customers. This links individuals as consumers with different degrees of economic value, and as citizens with different degrees of risk.

The UK's Money Laundering Regulations 2007 require financial institutions to notify "suspicious transactions" to the Serious Organised Crime Agency, who received 247,601 reports in the year to September 2011. Under the e-Borders scheme, shipping and aircraft companies electronically supply information on the 200 million passengers crossing the UK border each year, for matching against government security and immigration risk databases. The draft *Communications Data Bill* would require Internet Service Providers to store an even broader range of records than at present, and also enable communications records to be directly requested from websites such as social networking sites.

All of this surveillance activity in itself may have a limited immediate impact. Norris (2012) notes that one explanation of the limited criminological impact of CCTV is that most people are unaware of the presence of cameras, and that even when offenders are aware of its presence, alcohol or other drugs frequently impair their judgment. Most claim it makes no difference as to whether or not they would commit a crime.

Evidence on the impact of much greater levels of state surveillance is difficult to find, since there are few historical precedents. The German Democratic Republic (DDR) perhaps came closest, with one in 6.5 members of the population acting as informers for the *Ministerium für Staatssicherheit* or Stasi, contributing to 180km of files (Funder 2003: 57).

It is difficult to disentangle the impact of surveillance itself on East Germans' identity from the state terror inflicted using that information, but Pfaff (1996: 402) suggests "The citizens of the GDR adapted to the … regime enforced by the Stasi by maintaining the outward appearance of conformity and compliance. At the same time, however, the state failed to penetrate the private lives of individuals". Funder (2003) suggests that extreme levels of state surveillance reduced the ability of young people to establish their own identity, making them compliant or desperate, angry and subversive.

2.2 Individual resistance

There has been significant resistance to state surveillance by civil liberties and environmental activists (surveyed extensively by Bennett 2008), including through the practice of what has become known as "sousveillance". Activists use technologies such as video recording against the surveillance authority, holding a mirror to surveillers and asking: "Do you like what you see?" and thereby reducing power disparities. Systems like Google's prototype "Goggles" could provide some of this functionality, while at the same time gathering more data about the user.

Sousveillance can be a powerful tool for holding authority to account, as seen in the footage of police officers beating Rodney King in Los Angeles that sparked days of rioting, and more recently in the trial of a London police officer (acquitted of manslaughter) recorded pushing a protest bystander to the ground, who died shortly afterwards. Other examples include "customers photographing shopkeepers; taxi passengers photographing cab drivers; citizens photographing police officers who come to their doors; civilians photographing government officials; residents beaming satellite shots of occupying troops onto the Internet" (Mann, Nolan and Wellman 2003: 333-4).

Sousveillance technologies can help influence media narratives that in turn shape the identity of protestors. Newlands (2009: 2) suggests that the G20 Meltdown and Heathrow Climate Camp protestors successfully used sousveillance and new media to shape "the cultural perception of protest groups and the wider field of new social movements".

Sousveillance complements Marx's (2003) notion of "blocking, distorting, masking, refusing, and counter-surveilling", which is especially relevant for less powerful groups that lack resources to undertake political campaigns of resistance. Another example is a student group's use of "the cyber-synoptic infrastructure of the Facebook network" to organise an international protest in 2006 against the surveillance practices of that site (Sanchez 2009). Mann *et al*. (2003: 347) conclude that "There is an explicit 'in your face' attitude in the inversion of surveillance techniques that draws from the women's rights movement, aspects of the civil rights movement, and radical environmentalism… situated in the larger context of democratic social responsibility".

"Everyday resistance" is a less organised and political, day-to-day undermining of surveillance practices, such as the use of radar to detect speed cameras, or "losing" tagged equipment or staff badges. One study even found that "morally conflicted welfare administrators resist authorities by coaching recipients on ways to game the system" (Gilliom 2001).

As well as subverting control mechanisms, everyday resistance is used by individuals to "test boundaries, build sociality, and achieve dignity." Societies seem to react in different ways to such resistance: from vehement media criticism of "welfare fraudsters" (who may simply be focused on meeting basic needs of their children), to seemingly less concern over speeding drivers, to in some cases celebration of tax avoidance in countries that can ill-afford such tolerance (Gilliom and Monahan 2012: 405-408).

2.3 Social sorting

A broader concern about the development of new surveillance technologies is that they can lead to "social sorting", where discrimination and privilege are entrenched through the unplanned consequences of data gathering and analysis (Lyon 2001). The process of identity construction itself will be increasingly shaped by targeted advertising, search results and other types of online information presented to users based on surveillance of their previous browsing behaviour.

Many public and private sector organisations now use profiling to determine service levels for different customers. Employers and universities use information from social networking sites for selection and disciplinary purposes. Insurers and private healthcare providers use biographical and transactional data for checking claims and setting premiums. Law enforcement and intelligence agencies gather a wide range of data for prosecutions and counter-terrorism investigations. Studies in the US, UK and Italy have found that even well educated "digital native" university students have little idea about these potential consequences of sharing personal information on social networks.

In each of these cases there can be significant consequences for individuals, but also a potentially discriminatory broader effect if information about gender, ethnicity, religion, sexuality, social class and other categorical data becomes a factor in employment, insurance and criminal case decisions.

While anti-discrimination laws are intended to prevent overt discrimination, the notion of "actuarial fairness" in many countries allows decision-makers to take into account categorical data that is highly correlated to outcomes relevant to the decision. Men frequently pay higher driving insurance premiums but lower annuity purchase prices, since statistically they are more likely to make claims than women drivers and to live shorter lives than women retirees

(although a recent European Court of Justice judgment has challenged this practice within the EU). These statistical summaries of population group variables do not apply directly to individuals – but are increasingly used as if they did, becoming “stereotypes by a different name” without regard to the moral relevance of the category or the impact on justice (Gandy 2010: 35).

Decisions that are even indirectly influenced by categorical data can bias statistical associations that then reinforce such stereotypes. Gandy (2010: 38) gives the example of data used in some US states to justify more frequent police stops of black drivers “because of a belief that those drivers are more likely to be carrying contraband drugs”. Regardless of the validity of this belief across an entire population, such over-sampling is likely to produce a higher absolute number of convictions in this group – and hence be used to justify the action.

Data driven “predictive policing” software from companies such as IBM is already being used to direct police attention. Separately, young black men are hugely over-represented in the UK National DNA Database, because they are stopped proportionately much more frequently by police than other ethnic groups. In turn this will lead to a higher number of convictions of black men as DNA evidence is matched against the database, “justifying” the additional attention they receive from police.

While the designers of such decision-making systems have an opportunity to reduce overt discrimination by biased individuals, they may inadvertently perpetuate “the far more massive impacts of system-level biases and blind spots with regard to structural impediments that magnify the impact that disparities in starting position will have on subsequent opportunities” (Gandy 2010: 34). Automated surveillance can lead to automation of social representation, and the removal of the possibility for negotiation and contention (Graham and Wood 2003) – and for rehabilitation, redemption or change. Guzik (2009) describes predictive data mining, popular as a counter-terrorism tactic in the UK and US, as an extension of “future-oriented power” that “discriminates by design, designating certain groups as threats relative to others”.

3. Opportunities and risks of changed identity

Taken together, these developments in surveillance and privacy technologies are likely to have a number of effects on identity over the next ten years, related to interpersonal trust, social mobility and conformity/obedience, and political pluralism.

3.1 Distrust in personal relationships and technology

Control of information disclosure is an important part of managing personal relationships. Between partners and friends, controlled disclosure builds intimacy and trust, while the ability to tell "little white lies" can be essential to smooth over conflict. If new surveillance technologies do not come with adequate privacy features, this disclosure control will be damaged. This could erode social ties and potentially contribute to family breakdowns and fewer quality relationships.

The "peer-to-peer" surveillance enabled by social networking and location services could have a significant impact on individual behaviour and identity. Opinions held by significant others are vital to individuals' self-esteem, anxiety levels, and happiness. Having to hide aspects of identity that might damage those opinions creates tension and conflict. And when personal information is used in unexpected ways, which is frequently the case with the ubiquitous and invisible surveillance practices encountered online, this can cause strong negative emotional reactions from those affected (Adams and Sasse 2001) – damaging their trust in that technology.

3.2 Social mobility and cohesion

Private and public-sector surveillance and profiling will lead to individuals increasingly being offered differentiated products and services based on past behaviour, and to a more targeted exercise of power in areas such as criminal justice and social security (Anderson *et al*. 2009). Unless approached carefully, this could significantly reduce aspiration and social mobility. It may also cause a reduction in social cohesion, if levels of common experiences and the perception of equal treatment are reduced. Norris (2012: 258) warns that "the primary target of CCTV is the young male, often from an ethnic minority, displaying the visible symbols of working-class or youth subculture who, through passivity or activity, is deemed out of place in the consumption-orientated high streets and malls of the global urban landscape."

3.3 Conformity and stigma

The Internet has given individuals greater freedom to explore different identities, reducing constraints on finding information about and participating in online discussion with similar others (McKenna 2007). Greater surveillance could constrain such "potential" selves, and force the revelation of stigmatised identities and interest in fringe ideologies – as well as reinforcing feelings of isolation, difference and shame.

Of course, extremist ideologies that promote violence are of great legitimate concern to society (exemplified by Norwegian mass murderer Anders Behring Breivik's ultranationalist writings). It

will be critical for governments to ensure surveillance is targeted closely and not broadened to non-violent political or religious communities, who may feel stigmatised and consequently be less willing to cooperate with other law enforcement measures.

Surveillance technologies are already widespread in workplaces, including CCTV in remote working areas, location tracking systems, and performance monitoring tools such as keystroke logging or audio monitoring. Psychometric measures, drug and alcohol tests are already common in US companies. These all make it easier for managers and colleagues to monitor employees' performance and compliance with rules and organisational norms, values and expectations (Sewell 2012).

As these systems become cheaper they may become even more widely deployed, including in professions that traditionally allow much greater levels of autonomy. Their deployment may also be driven by the increasing number of teleworkers, many of whose managers will be used to working in the same physical location as their staff. While these tools may improve organisational performance and in some cases protect worker safety, they are also likely to have a negative impact on employee autonomy and creativity.

3.4 Judgment by authority

While the use of privacy technologies (such as e-mail encryption) remains relatively unusual, users could be wrongly identified with those attempting to hide criminal activities. Conversely, the UK Security Service (MI5) warned during the parliamentary debate on the Digital Economy Act 2010 that measures to require ISPs to monitor user traffic for copyright infringement could encourage wider use of encryption, which would make it more difficult for MI5 to put serious criminal suspects under surveillance. The success of the Pirate Party in several European elections seems to be partly due to its pro-privacy platform, and particularly its rejection of copyright enforcement measures that require greater levels of Internet surveillance.

Broader law enforcement use of new surveillance technologies also runs the risk of damaging the public acceptance central to the UK notion of "policing by consent". Wells and Wills (2009) found that speed enforcement cameras challenge many UK drivers' self-identity as respectable and non-criminal; they instead feel unfairly characterised as "risk-carrying, deviant, and criminal" – generating a sense of injustice and encouraging resistance. This included a rejection of the evidence used to justify such surveillance, and the creation of a narrative of ordinary drivers resisting an oppressive state, whose attention should be focused on other more "genuine" deviants such as violent criminals and other "familiar folk devils". This was despite widespread evidence that speed cameras have significantly improved road safety and reduced traffic deaths.

3.5 A plural society

Surveillance can have a significantly constraining effect on political debate and protest, and hence reduce the broader public debate on socially contested issues, and the ability of weaker groups to resist power. As the German Constitutional Court noted in a 1983 judgment: "a person who wonders whether unusual behaviour is noted each time, and thereafter always kept on record, used or disseminated, will try not to come to attention in this way ... This would ... limit the ... common good, because self-determination is an essential prerequisite for a free and democratic society that is based on the capacity and solidarity of its citizens." The idea of "panopticism" is that surveillance "fosters well-adapted, peaceful, disciplined behaviour" and

ultimately deters demonstrations and other disorderly behaviour (Ullrich and Wollinger 2011: 27).

Despite the technological opportunities for sousveillance, Ullrich and Wollinger (2011) note that power asymmetries remain for protestors. Police are “better equipped, outfitted with public legitimacy, more trusted by courts, in possession of other preventive and repressive instruments,” and can also seize protestors’ recordings for their own use (Ullrich and Wollinger, 2011: 24). They conclude that “a technical arms build-up of open and concealed surveillance… signals the encroachment of authoritarian concepts of the state and is a potentially dangerous attack on political participation from below” (p.33).

References

Adams, A. and Sasse, M.A. (2001) *Privacy in Multimedia Communications: Protecting Users, Not Just Data*. In Blandford, A., Vanderdonkt J. and Gray, P. (eds.) People and Computers XV - Interaction without frontiers. Springer, 49–64

Anderson, R., Brown, I., Dowty, T., Inglesant, P., Heath, W. and Sasse, A. (2009) *Database State*. Joseph Rowntree Reform Trust: York, UK

Askoxylakis, I., Brown, I., Dickman, P., Friedewald, M., Irion, K., Kosta, E., Langheinrich, M., McCarthy, P., Osimo, D., Papiotis, S., Pasic, A., Petkovic, M., Spiekermann, S. and Wright, D. (2011) *To log or not to log? - Risks and benefits of emerging life-logging applications*. European Network and Information Security Agency

Bennett, C. (2008) *The Privacy Advocates.* MIT Press: Cambridge, USA

Bohme, R. and Koble, S. (2007) *On the Viability of Privacy-Enhancing Technologies in a Self-Regulated Business-to-Consumer Market: Will Privacy Remain a Luxury Good?* Proceedings of the Workshop on the Economics of Information Security

Brown, I. (2012) *Government Access to Private-Sector Data in the United Kingdom*. International Data Privacy Law, 2(4), forthcoming.

boyd, d. (2008) *Why Youth ❤ Social Network Sites: The Role of Networked Publics in Teenage Social Life*. In David Buckingham (ed.) Youth, Identity, and Digital Media. MIT Press: Cambridge, USA, 119–142

Cooley, C.H. (1902) *Human nature and the social order.* Scribners: New York

Funder, A. (2003) *Stasiland*. Granta Books: London

Gandy, O. (2010) *Engaging rational discrimination: exploring reasons for placing regulatory constraints on decision support systems*. Ethics and Information Technology 12(1) 29–42

Gill, M. and Spriggs, A. (2005) *Assessing the impact of CCTV*. Home Office Research, Development and Statistics Directorate, 43, 60–61

Gilliom, J. (2001) *Overseers of the Poor: Surveillance, Resistance, and the Limits of Privacy*. University of Chicago Press: Chicago

Gilliom, J. and Monahan, T. (2012) *Everyday resistance*. In Ball, K., Haggerty, K., and Lyon, D. (eds.) Routledge Handbook of Surveillance Studies. Routledge: Abingdon, UK, 405–412

Goffman, E. (1959) *The presentation of self in everyday life.* Doubleday Press: New York

Graham, S. and Wood, D. (2003) *Digitising surveillance: categorisation, space, inequality*. Critical Social Policy, 23(2), 227–248

Guzik, K. (2009) *Discrimination by Design: Data Mining in the United States's 'War on Terrorism'*. Surveillance and Society, 7(1), 1–17

Hildebrandt, M. (2008) *Profiling and the identity of the European citizen.* In Hildebrandt, M. and Gutwirth, S. (eds.) Profiling the European Citizen. Springer: Netherlands, 303–343

Hogan, B. (2010) *The Presentation of Self in the Age of Social Media: Distinguishing Performances and Exhibitions Online*. Bulletin of Science, Technology and Society, 30(6), 377–386

Joinson, A.N. and Paine, C.B. (2007) *Self-disclosure, privacy and the Internet*. In Joinson, A., McKenna, K, Postmes, T and Reips, U.-D. (eds.) The Oxford Handbook of Applied Psychology, Oxford University Press: Oxford, 237–252

Lianos, M. (2003) *Social Control after Foucault*. Surveillance and Society, 1(3), 412–430

Livingstone, S. (2006) *Children's Privacy Online: Experimenting with boundaries within and beyond the family*. In Kraut, R., Brynin, M. and Kiesler, S. (eds.) Computers, Phones, and the Internet: Domesticating Information Technology. Oxford University Press: Oxford, 128–144

Lyon, D. (2001) *Surveillance Society: Monitoring Everyday Life*. Open University Press: Buckingham, UK

Mann, S., Nolan, J., and Wellman, B. (2003) *Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments*. Surveillance and Society, 1(3), 331–355

Marwick, A., Murgia Diaz, D. and Palfrey, J. (2010) *Youth, Privacy, and Reputation*. Harvard Public Law Working Paper No. 10-29

Marx, G. (2003) *A Tack in the Shoe: Neutralizing and Resisting the New Surveillance*. Journal of Social Issues, 59(2), 369–390

McKenna, K.Y.A. (2007) *Through the Internet looking glass: Expressing and validating the true self*. In Joinson, A., McKenna, K, Postmes, T and Reips, U.-D. (eds.) The Oxford Handbook of Applied Psychology, Oxford University Press: Oxford, 205–222

Mead, G.H. (1932) *Mind self and society from the standpoint of a social behaviorist*. University of Chicago: Chicago

Moinian, F. (2006) *The Construction of Identity on the Internet: Oops! I've left my diary open to the whole world!* Childhood, 13(1), 49–68

Nissenbaum, H. (2010) *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press: Palo Alto

Norris, C. (2012) *The success of failure: Accounting for the global growth of CCTV*. In Ball, K., Haggerty, K., and Lyon, D. (eds.) Routledge Handbook of Surveillance Studies. Routledge: Abingdon, UK, 251–258

Pfaff, S. (1996) *Collective Identity and Informal Groups in Revolutionary Mobilization: East Germany in 1989*. Social Forces, 75(1), 91–117

Sanchez, A. (2009) *Facebook Feeding Frenzy: Resistance-through-Distance and Resistance-through-Persistence in the Societied Network*. Surveillance and Society, 6(3), 275–293

Sewell, G. (2012) *Organization, employees and surveillance*. In Ball, K., Haggerty, K., and Lyon, D. (eds.) Routledge Handbook of Surveillance Studies. Routledge: Abingdon, UK, 303–312

Ullrich, P. and Wollinger, G.R. (2011) *A surveillance studies perspective on protest policing: the case of video surveillance of demonstrations in Germany*. Interface, 3(1), 12–38

Wells, H. and Wills, D. (2009) *Individualism and Identity Resistance to Speed Cameras in the UK*. Surveillance and Society, 6(3), 259–274

Westin, A. (1999) *IBM-Harris Multi-National Consumer Privacy Survey*

Acknowledgments

Many thanks to Grant Blank, Bernie Hogan, Adam Joinson, Mark Levine, Judith Rauhofer, Angela Sasse, Ralph Schroeder and the anonymous reviewers for their help.

© Crown copyright 2013
Foresight
1 Victoria Street
London SW1H 0ET
www.foresight.gov.uk
URN 13/507