

**“EVERY BREATH YOU TAKE, EVERY MOVE YOU MAKE, I’LL
BE WATCHING YOU:” THE SOCIAL IMPACT OF SURVEILLANCE
TECHNOLOGY**

DR. HAZEL LACOHEE

*BT Group Chief Technology Office, Adastral Park, Martlesham Heath,
Ipswich, UK.
hazel.v.lacoe@bt.com*

AND

DR. ANDY PHIPPEN

*Information Security and Network Research Group, School of
Computing, Communications and Electronics, University of Plymouth,
Drake Circus, Plymouth, UK.
andrew.phippen@plymouth.ac.uk*

Abstract. The past decade has brought unprecedented developments in technology and these increasingly impact on our daily lives. Technological advances define how we live; from how we communicate and are entertained to how we access government services. In order to understand technology adoption and acceptability it is important to consider how the technology fits with and supports human endeavours and activities. We report findings from the Trustguide project (Lacoe et al, 2006) that took a “citizen-centric” approach to exploring issues of trust, security and privacy in ICT based applications and services covering a broad a spectrum UK citizens.

1. Introduction

Privacy and the potential impact of technological advances on the private sphere of day to day life is the “big issue” that we need to address. Current citizen attitudes would suggest an informed society who have strong views regarding surveillance technologies. This could potentially have significant impacts upon the trust relationships that exist between a state and its citizens.

2. Surveillance society

Modern technology has inevitably resulted in a surveillance society where almost every activity of our daily lives can be tracked and traced. Indeed, it has become so routine as to have become almost unnoticeable in many respects. In November 2006 the Information Commissioner Richard Thomas introduced 'A Report on the Surveillance Society' (Ball et. al., 2006), specially commissioned for the 28th International Data Protection and Privacy Commissioners' Conference. It opens with a statement of fact: 'We live in a surveillance society. It is pointless to talk about surveillance society in the future tense.' We encounter surveillance technologies on a daily basis, whether we are aware of them or not, from CCTV capturing our everyday movements on the streets, in shops and car parks to tracking of purchasing via loyalty and credit cards. Public surveillance is highly pervasive and likely to accelerate in the future as technological advances make it increasingly easy to monitor activities and gather large quantities of data concerning individuals' daily lives. But what is a surveillance society, what impact does this have on our lives and what impact might it have in the future?

In the context of this paper the most appropriate definition of a surveillance society is one where technology is extensively and routinely used to track and record our activities and movements. This includes systematic tracking and recording of travel and use of public services, automated use of CCTV, analysis of buying habits and financial transactions, work-place monitoring of telephone calls, email and internet use and collection of personal and health data.

For the purpose of this paper we will concentrate on two forms of public surveillance; mass visual surveillance, and mass informational surveillance. Mass visual surveillance relates to the use of CCTV and road user charging systems including congestion charging. It is usually undertaken as 'background' rather than targeted activity and is claimed, particularly in the case of CCTV, to have crime prevention benefits. Individuals cannot refuse consent to the recording of their image and may or may not be aware that they are being filmed. Mass informational surveillance is related to databases, including government-led initiatives, requiring collection, retention and use of information such as the National Identity Register (NIR), the Children's Index and the National Health Register. What these forms of surveillance have in common is the potential to infringe human rights and undermine trust. The bodies set up to collect such data, and the justifications provided for such necessity, may alter the relationship between the citizen and the state and seriously impinge on privacy.

3. Public Perceptions of Mass Visual Surveillance

The UK has the highest level of public surveillance in the world (Frith, 2004); more than four million surveillance cameras monitor our movements in the streets, shops, banks, hospitals, car parks, railway stations, and the London underground (that alone operates 1400 cameras). Although much of this activity centres on security, crime detection and prevention and hence can be seen as serving society, we found high levels of public concern in our discussion groups regarding what is perceived as heavy surveillance and tracking of day-to-day activity:

“There’s people watching me doing ordinary, every day activities which I consider as entirely private.”

“It is corrosive, being watched when we don’t know and feel we’re being watched, it has a very different psychological effect than being watched when you know you’re being watched.”

Clearly being watched can be corrosive, Hookway (2000) introduced the concept of the panspectron to describe the use of CCTV surveillance to record activity in public places i.e. the case where no particular surveillance subject is identified, instead information is collected about everything and everyone all the time. A subject appears only when a particular question is asked, thus triggering data mining in information already gathered to learn what can be gleaned in answer to that question. While in the panopticon environment (Foucault, 1979) the subject knows that the watcher is there, in the panspectron environment one may be completely unaware that information is being collected at all (Brahman, 2006). We found that many attendees were highly distrustful of such surveillance measures and felt that they infringed civil liberties. The effect of this is that it leads to a reciprocal lack of trust between the citizen and the State:

“It means I can’t travel from A to B in this country without a central computer logging my movements, I mean not an audit trail which somebody could dig into if they needed to if there had been a mass murder or something, but the idea that there is a central computer somewhere that knows exactly where I am. Effectively that’s infringing on my freedom.”

Attendees were also distrustful of justifications for increased surveillance (e.g. control of terrorist activities, reducing crime) and this tended to decrease any sense of belief in public benefit:

“A lot of this stuff is being hyped up and marketed to us as ‘this will solve our terrorism problem.’ Actually there’s two things about that. One, we know is who is to blame but it will not solve the problem they’re telling us it’s going to solve and

so that reduces your trust. The second is that in any event, all of this stuff has to be after the fact, it is not prevention.”

Our discussions revealed that levels of surveillance are perceived to have increased in recent years with, for example, the enforcement of the London Congestion Charge (Transport for London, 2007) and automatic car registration recognition camera systems. Many attendees found this unwelcome and were highly aware of how extensions of these technological capabilities might lead to function creep:

“If your vehicle is being tracked from A to B they measure the time, they say ‘taking your average speed, you must have been speeding at some point’ and that to me is an application where it stops people thinking. The brain is like a muscle, the less you exercise it the less intelligent we become as a society. The effect of having more things done for us automatically is that it becomes positive aggression. This speeding application means that you’re not thinking about safety, it all done for you.”

As well as taking away individual responsibility for obeying the law such activities were seen by attendees as having far reaching implications for civil liberties and privacy, particularly in terms of how CCTV footage might be used by those other than the original gatherers of such data and a strong need for improved legislation was voiced:

“I don’t think there’s any law that stops my local petrol station for example sharing CCTV footage with anyone else who might be interested in it.”

For most such levels and operation of surveillance techniques were perceived as extreme and many felt they were detrimental to societal values because they encroach on the private sphere of life and diminish a sense of control:

“It’s the loss of a sense of control over a private sphere that I most dislike, not because I have anything to hide but because it is a private sphere and it has a meaning in the sense of self to my children and to me and my wife. I think that is a very deep loss, the sense of a private sphere.”

This emphasises the importance of the private sphere of life and the need to ensure that technological advances support rather than undermine societal values.

3.1. PROFILING STATISTICAL NORMS OF BEHAVIOUR

Impersonal and rule-centred practices have contributed to the proliferation of public surveillance. Of particular concern was the notion that behaviour could be monitored to identify those that fail to fit a statistical norm or

standard behavioural pattern. Such techniques are generally employed to identify threatening, damaging or criminal behaviour. Attendees felt that reducing behaviour to a mathematical probability was vulnerable to erroneous inference and results in an increased sense of guardedness and a decreased sense of individual freedom:

“You have to spend your time second-guessing what a system written by somebody who had to write a rule somewhere is going to make of what you’re doing. For example there are smart surveillance systems that the railways use that detect people who are likely to throw themselves under a train. They detect that if you stand on the same spot and two trains go by you are at risk of suicide and they will send a security guy down. It’s the same software that looks for rectangular objects sitting still in an airport lounge. That software is getting very, very smart and what it comes down to is statistical behavioural odds. If you just happen to feel like sitting there day dreaming, say I’m Keats and composing something, then I’m likely to be interrupted by this guy trying to save my life when I had no intention or thought of suicide anyway.”

The long-term impact of behavioural profiling was perceived to pose particular and unprecedented problems having far reaching societal implications. It also reveals evidence of a perceived mismatch between government and commercial interests and those of the public at large:

“For years now I’ve monitored what I write in emails because I know that everything written in email persists forever. Now you think of a world where kids grow up and throughout their childhood and adolescence everything they ever did or said, or where they went, or who they associated with, and what they bought is a matter of record...I don’t know how we stop it but we certainly can’t stop it without a huge amount of effort to make things anonymous.”

It can be argued that collecting and retaining information about the everyday movements of average law-abiding citizen is an infringement of their right to privacy unless explicit consent has been provided or there is a strong justification e.g. public safety, and any surveillance measures employed have strong, proven efficacy. If technologies continue to be developed and employed with the intention of monitoring large numbers of people they are likely to intrude increasingly into the lives of ordinary citizens who in turn will increasingly find cause to object.

4. Public Perceptions of Mass Informational Surveillance

The creation of mass information, large scale databases raises issues similar to those concerning mass visual surveillance; however, since electronic capture and storage of valuable personal details are at stake here concerns regarding security are high on the agenda. The majority of our attendees wholly dismissed the concept of a totally secure system, not least because it requires a human element in order to function and this is perceived as the weakest link in security:

“The technology could be the downfall, or people operating it could be the downfall, even if you have got a security policy in place, it doesn’t mean someone can’t break it.”

Personal data protection is a matter of increasing concern to UK citizens but those concerns are often ill-defined; we found high levels of uncertainty concerning what data is held, by whom, how securely it is stored, shared or amalgamated, who has access to it and under what circumstances or indeed, how individuals might be better informed about such matters and what their rights are in this respect. Similar findings were reported by Mori (2003) which suggests that little has changed in the recent years and people are no better informed. The ability to hold mass information via large scale electronic data bases is a relatively new phenomenon to the average citizen and represents one of the most significant societal changes of recent years (Crossman et. al., 2007). Undoubtedly one of the strongest arguments in favour of a national identity register is that it will improve public security but our discussions reveal that citizens perceive the collection and storing of such data as increasing vulnerability rather than increasing security:

“I feel more vulnerable having all my data like personal details held in one place electronically than I would having ten separate paper documents held in different places.”

Our findings are supported by a recent YouGov poll (2007) commissioned by the human rights group Liberty (2007) who found that only seventeen percent of Britons trust the authorities to keep their personal details completely confidential and fifty seven percent believe the UK has become a surveillance society. There is a strong belief amongst citizens that personal information about them does belong to them rather than the bodies who collect, use and process that data.

5. Conclusion

Respect of citizens’ rights to a private life is vital to human dignity. A citizen’s right to privacy is infringed unless they have explicitly consented to data being collected or there are proven, open, honest and strong

justifications for such infringement. Surveillance technologies, however well-intentioned, have the potential to undermine societal values and societal cohesion and to upset the balance between society and State. This is most in evidence where data is collected covertly, without citizens’ consent or knowledge, where they have no option to ‘opt out’ and no control over how the data is used, sold, stored, or amalgamated with other data. Such an imbalance of power can be redressed by introducing reciprocity into the relationship between citizens and any given surveillance agency by ensuring that data is not collected excessively, is appropriate, not intrusive, and provides an option to make complaints to an independent body. It is imperative that surveillance technologies should be deployed in a responsible manner, under strict supervision, and with increased levels of public accountability and individual rights of redress for mistakes. This should be supported by a legally enforceable code of conduct and regulations, and clear explanations as to the proven benefits and advantages of current and/or increased levels of public surveillance.

In order to achieve an effective balance that does not intrude on the private sphere of life surveillance measure should be in the interests of and show clear benefits to the citizen. Blanket surveillance benefits should not outweigh any impact on privacy hence justifications must be clear, open and honest. Any centralised collection and storage of personal data, especially one that is justified by, in the opinion of citizens, unrealistic claims of security and protection, is likely to be greeted with distrust. We suggest that the relationship may be enhanced where the attendant risks and vulnerabilities are effectively managed and there is mutual understanding and a clear vision of benefit for both parties, choice about what data is stored, increased anonymisation and realistic and achievable guarantees of restitution when something goes wrong.

A society which does not pay sufficient regard to personal privacy is one where dignity, intimacy and trust are fatally undermined (Crossman et. al., 2007). Citizens are likely to react most strongly where measures (and mistakes) impact on the private sphere of life. Mass surveillance schemes should be appropriate and proportionate to the problems they set out to solve and should minimise intrusion. Consent must be sought where appropriate and there must be greater clarity concerning what information is held about individuals by whom, with clear audit trails to provide greater transparency to the individual in tracing how their data is being used.

References

Ball, K., Lyon, D., Murakami Wood, D., Norris, C. and Raab, C.: 2006, *A Report on the Surveillance Society*, [online]

- http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf
- Brahman, S.: 2006, *May Tactical Memory: The Politics of Openness in the Construction of Memory*, *First Monday* Conference, May 2006, [online] <http://www.firstmonday.org/>
- Crossman, G., Kitchin, H., Kuna R., Skrein M., and Russel, J.: 2007, *Overlooked: Surveillance and personal privacy in modern Britain*, [online] www.liberty-human-rights.org.uk/issues/3-privacy/pdfs/liberty-privacy-report.pdf
- Delgado, M., Ludgate, R., and Nicol, M.: 2007, *DVLA sells your details to criminals*. *Mail on Sunday newspaper*, 12th February 2007. [online] http://www.mailonsunday.co.uk/pages/live/articles/news/news.html?in_article_id=369838&in_page_id=1770&in_page_id=1770&ct=5&expand=true
- Foucault, M.: 1979, *Panopticism*, In: *Discipline and punish: The birth of the prison*, Translated by Alan Sheridan, Vintage Books, New York, pp. 195–230.
- Frith, M.: 2004, *Big Brother Britain 2004*, *Independent newspaper*, 12th January 2004, [online] <http://newsmine.org/archive/security/britain-4m-cctv-surveillance-cameras.txt>
- Hookway, B.: 2000, *Pandemonium: The rise of predatory locales in the post-war world*, Princeton Architectural Press, Princeton, N.J.
- Lacoehee, H., Crane, A, and Phippen, A.: 2006, *Trustguide Final Report*, [online] <http://www.trustguide.org.uk>
- Liberty: 2007, *Human Rights group*, [online] <http://www.liberty-human-rights.org.uk/>
- Matthieson, S.: 2007, *UK government loses data on 25 million Britains*, *Computer Weekly*, 20 November 2007, [online] <http://www.computerweekly.com/Articles/2007/11/20/228216/uk-government-loses-data-on-25-million-britons.htm>
- Mori Poll: 2003, *Privacy and Data-Sharing: Survey of Public Awareness and Perceptions*, [online] <http://www.dca.gov.uk/majrep/rights/mori-survey.pdf>
- Randerson, J.: 2006, *DNA of 37% of black men held by police*, *Guardian newspaper*, 2006, Thursday January 5th, [online] <http://www.guardian.co.uk/frontpage/story/0,16518,1678168,00.html>
- Transport for London: 2007, *Congestion charging payment information*, [online] <http://www.cclondon.com/paymentinformation.shtml>
- UK Home Office: 2007, *The national DNA database*, [online] <http://www.homeoffice.gov.uk/science-research/using-science/dna-database/>
- YouGov: 2007, [online] <http://www.yougov.com/> Online survey, total sample size 2,500 adults