

# Privacy, Identity and Crime Prevention

**Michelle Rogerson and Ken Pease**  
**University of Huddersfield**

---

**This is a short review document covering a number of issues relevant to the Cyber Trust & Crime Prevention project. While the Office of Science and Technology commissioned this review, the views are those of the author, are independent of Government and do not constitute Government policy.**

## 1 INTRODUCTION

Privacy, identity and protection from crime are complementary goals, each a human right to be safeguarded. Moreover crime prevention provides a means to protect citizens from infringements to privacy and threats to identity. At face value a conflict between these goals is not apparent. Relinquishing rights to liberty, privacy and control over one's identity as punishment for wrong doing has a long history in the form of incarceration. This form of crime prevention<sup>1</sup> targets a specific individual for the *proven commission of a specific offence*. Although there will always be grounds for contention around what constitutes a crime, the contradictions between crime prevention, privacy and identity become most difficult when crime prevention interventions cast their net more widely.

Routine Activity Theory (see Felson (1987)) encourages crime preventers to consider the (physical and virtual) locations and times in 'everyday life' when motivated offenders come into contact with vulnerable crime targets in the absence of capable guardians. Crime prevention activity should focus upon manipulating the world to prevent this 'conjunction of criminal opportunity' (Ekblom (2000)). However the routine activities of offenders take place in the same spaces as the activities of other members of society. Manipulating the world for offenders alters the world for the rest of the population. The extent to which interventions impact solely on the offender, or more widely, varies across interventions and with the nature of their implementation.

Social change in late modern society has changed the nature of trust (Giddens (1990)), the role of the intermediary has been eroded and trust is now placed in complex systems rather than individuals. Access to premises, systems and services is increasingly dependent upon proof of identity. Current solutions involve a multitude of documents, plastic cards, PIN numbers and passwords to carry and remember (or to lose and forget). These are all forms of identity that can be performed without the body, they are only effective if they are a secret known only to the user, identity has become valuable in its own right and is increasingly vulnerable to identity theft. Consequently proof of identity must be increasingly sophisticated.

## 2 IDENTITY

Identity is fluid; we each have different aspects to our identity, presented in different contexts. Concerns about the protection of identity focus on the right to control how much of our identity we reveal, and the right to choose anonymity. A key question is how much information about our identity is required for crime prevention purposes? Is it becoming harder to protect our 'identity' when we are called upon to reveal it so frequently?

Supporters of a UK identity card report that around 90% of the population already carry identifying information on plastic cards and argue that an ID card is no different, in fact it may prove more convenient enabling less cards to be carried. Currently card holders exercise 'informed consent' regarding which cards they carry and when. On the other hand an ID card could be mandatory,

---

<sup>1</sup> Although crime prevention and punishment are often separated imprisonment prevents crimes potentially commit were the offender at liberty and aims to deter future crimes.

and for some groups would have to be in order to access services. The convenience of more information on one card also raises concerns of 'functional drift' whereby a card used for a multitude of functions will link together different pieces of information about our identity. While we consent to reveal a 'piece of ourselves' in one context in another the same information could be irrelevant, inappropriate or embarrassing. Date of birth may be relevant information for receipt of pensions; in other contexts we may not wish to disclose it. The potential for commercial interests to use an identity card, for example in place of separate cards in loyalty schemes, raises further concerns about who knows what about us.

### 3 DATA USAGE

Technology has facilitated the fast and efficient processing and storage of large volumes of information. Data Protection legislation aims to ensure consent for data storage, assurances that data collected are necessary and provisions against the matching of personal records across different sources, such as health and insurance records with police data. Matching of information can paint a picture of lifestyles or business activities on which judgements can be made, be they judgements of criminality, or of a marketing target. Assurances against the secondary use or linkage of personal data can and have to be made but campaigners have insufficient trust in those managing databases and are aware that assurance from future responsible authorities are unobtainable now.

The vast majority of services we use, both in and out of cyberspace, compile and store personal data. Further web sites and services make access to services dependent on the provision information, effectively circumnavigating informed consent. Opting out of transactions we perceive as risky may become harder as more services move into the electronic arena. Legislation limited to State boundaries is futile in cyberspace and data protection and privacy are not even topics of note in many Asian countries. Data capture can be unsolicited when for example 'cookies' or Active X collect information about the websites we visit, potentially correlating information across different websites, not one of the most frequently used websites meet basic privacy standards (Electronic Privacy Information Centre (1997)). Cookies can be disabled but most people do not have the technical knowledge to manage these technologies. Public concerns over netcrime have not inhibited the expanding use of the Internet. Users are either in a happy state of ignorance or they are keeping their fingers crossed while they enjoy the new convenience and new benefits. Most are unaware of firewalls and other protection mechanisms. There is clearly a risk that protection of privacy and identity may become increasingly restricted to those with the technical capacity and know-how.

### 4 BIOMETRICS AND ENCRYPTION

The use of biometrics, unique measurable human characteristic used to automatically recognise or verify an identity, have also raised fears about the linking of information sources. Biometrics unquestionably tie individuals to their identity<sup>2</sup>, depriving them of the right to anonymity. The solution may lie in the specific application of the technology. Biometric encryption/decryption enables security to be combined with privacy. The iris, or other measures, can be used to encrypt passwords or PINS, the biometric itself is only stored naturally on the user, leaving no unique identifier stored in linkable databases. The user can have a multitude of passwords protecting different aspects of identity for different purposes, (strength in diversity) but the need to remember them all is also removed with the biometric technique.

As with other identity protecting technologies, (e.g. encryption, digital signatures, digital pseudonyms and anonymous remailers) encryption is also proving extremely valuable for those involved in criminal activity. Computing capacity is exponentially increasing the power and complexity of the ancient tool of encryption. Encryption of communications conducted over insecure networks enables those subject to human rights abuses to communicate freely, whistle blowers to report unfair work practices, financial transactions to be conducted securely and confidential business data to be kept secret. The technology however is also available for

---

<sup>2</sup> Although biometric software may work within a margin of probability defined by programmers

criminals, and terrorists. This has led Governments, notably the US, to attempt to impose legal limits on the strength of encryption or the compulsion to surrender of decryption keys by law. Other suggested solutions include the use of 'recoverable encryption' relying on trusted third parties to hold decryption keys. Limiting the use of encryption for criminals also limits its use for others including those with crime prevention objectives. Furthermore regulation of encryption will always prove inadequate not least because offenders will find the risk of conviction under encryption laws more favourable than those for e.g. white-collar crime, drugs trafficking or terrorism. Not all criminal cases involving encrypted documents have required decryption. Authorities have obtained keys by other means, found hard copies of the information or unencrypted files and not all criminal communications are encrypted, and at present most child pornography is not encrypted. There are also other methods to keep a secret. Most are easier to crack, but their use can be harder to detect. These include stenography, hiding messages within other files and storing incriminating evidence on others' servers. Those attacking encrypted services have done so not by beating the encryption but by, for example, deceiving users into providing their account details. Excessive focus on limiting encryption may be at the expense of more effective, yet less intrusive, crime prevention interventions.

## 5 CCTV

Excessive focus on CCTV surveillance and unimaginative implementation may have contributed to the concerns associated with the extension of its use. CCTV has a wide range of applications; Von Hirsch (2000) has described three types of CCTV deployment each of which involves an increasing degree of intrusion. He recommends that CCTV should be limited to the tracking of activity within a specific location over time, providing a record of activity for inspection when and only when an offence is known to have taken place. Intrusion to privacy is minimised, restricted only to those locations and times in which offences have occurred. However, most CCTV systems in place today already go further than this. The problem is that beyond a limited deterrent effect, reliance on recorded images is not an effective method of crime prevention. Unreported crimes will go unmonitored, and there is no attempt to intervene in crime events prior to their occurrence.

Constant surveillance in real time carries greater potential to intervene in a crime, but also involves a greater intrusion of privacy. It is suggested that the locations surveyed in this way should be clearly publicised enabling the watched to manage their identity appropriately. This does not conflict with crime prevention aims which rely upon the offender's increased perception of the risk of offending. Real time CCTV monitoring will also catch those without criminal intent in its gaze. Von Hirsch and others have argued that crime prevention benefits need to be sufficiently high to justify this invasion of privacy, and should directly benefit those being monitored. Consequently, this form of monitoring should only be used in locations with a high crime risk. He provides the example of a bank cash machine. Under this principle a retailer wishing to defend her stock against shoplifters could not justify the surveillance of all customers as they would not directly benefit. Again, there is some conflict with effective crime prevention. Offenders are not necessarily specialists, and those who commit serious offences are also likely to commit minor crimes and infringements. Targeting those committing more minor, less damaging, offences may be a more effective means to pick up a bank-robber than pointing a camera at a bank and waiting for someone to decide to rob it.

Despite concerns, acceptance of CCTV in the UK is fairly widespread to the point that communities often demand it. CCTV gained popularity as a crime prevention mechanism, and is perceived as cost-effective by government, although its effectiveness in certain contexts has recently been placed in some doubt (Brandon et al (2002)). Advocates suggest that 'if you are not doing something wrong you have nothing to worry'. However this assumes a consensus over what constitutes acceptable behaviour. Political demonstrators may well disagree as might those caught by speeding cameras. Palmer (2000) has argued that we have created ever more vigilant self-policing with people aiming to avoid being misrecognised as a criminal.

The third level of CCTV operations involves the use of advanced capabilities to zoom in on and track individuals on the basis of the characteristics or their behaviour. For example, humans or software can identify recognised faces, suspicious behaviour or potentially criminal 'gait'. This raises a question central to the ethics of crime prevention of how crime prevention is deployed and

whether class or other sectional interests shape the direction and extent of work designed to prevent crimes. Sports fans have been 'scanned' on entry to sports stadia and cross-matched with databases of known and wanted criminals and terrorists. Are the crime risks to genuine sports sufficiently high to warrant the screening of all faces and what is the risk of generating a 'false positive'? On the other hand, given that humans are actually quite poor at facial recognition, is recognition software a more effective means to prevent crime to the overall safety and benefit of those attending?

Facial recognition systems operational in a London borough raised criticism for storing both matches and 'near matches' resulting in the expansion of offender databases to include those who look a bit like offenders. The National DNA database is now regulated to store the DNA of those who have been arrested and charged although not necessarily convicted. Those who come to police attention are statistically more likely to commit an offence in the future. A statistical likelihood of offending is very different from the commission of an offence, while prediction remains far from perfect. Is it fair to use this broad brush approach?

Are individuals the only focus for CCTV? Systems under development<sup>3</sup> discriminate changes in an overall visual scene aiming to spot changes from the norm, an individual behaving out of the ordinary may trigger the alert but other individuals will be literally ignored by the system. Would less intrusive alternatives be more effective? Street lighting has been shown to be more effective than CCTV in some contexts.

## 6 CRIME PREVENTION

Crime will never be eradicated from society and some definitions of crime prevention, refer to the reduction of crime to 'tolerable levels' (Ekblom (1996)). Kleinig (2000) argues that we must tolerate whatever level of crime we cannot diminish without incurring unacceptable social developments and more costs. The point at which intrusions to privacy and threats to identity are not balanced by benefits in reduced crime should mark the boundaries of this tolerable level.

Criminology desperately needs to get to grips with the future in order to anticipate and prepare for crime changes. However there are, at least, two dangers in prediction. Forecasting potential crime threats can produce dramatic scenarios that can encourage the development of heavy-handed solutions. What degree of effort should be directed towards the 'worst case' scenario compared to the 'most likely' scenario? The two may be very different. Many risks are plausible but hyped (Levi (2001)), and amplification of risks can be manipulative. The imperfections of predicting human behaviour should instil caution. At what point does a *statistical likelihood* of offending warrant *treatment as an offender*? Having done his/her time how comparable are the rights of ex-offenders to those of other citizens? On the other hand, should law-abiding citizens accept to be treated as fundamentally untrustworthy until proven otherwise?

Despite the availability of advanced ICT many crimes (types of credit card fraud) and threats to privacy, remain relatively low tech, and many successful solutions will be similarly low tech. Consequently, we need to avoid technological determinism and over-reliance on single solutions. Technology is not a runaway force, solutions will be found in novel twists to existing and emerging technologies in addition to the increased use and effectiveness of technologies that are currently the root of contention. Moreover, solutions must have proven effectiveness, there are countless examples of security measures that are not only intrusive but ineffective to boot.<sup>4</sup> Effectiveness should not be the sole criterion; we need ethical standards as well as empirical evidence.

---

<sup>3</sup> For an example see [www.dcs.qmul.ac.uk/research/vision/projects/ICONS/](http://www.dcs.qmul.ac.uk/research/vision/projects/ICONS/) (accessed 1 Nov. 03).

<sup>4</sup> <http://www.privacyinternational.org/activities/stupidsecurity/> (accessed 1 Nov. 03).

## Notes and references

Brandon C. Welsh and Farrington, D.P (2002) 'Crime prevention effects of closed circuit television: a systematic review', Home Office Research Study 252, London.

Eklom, P (1996) 'Towards a Discipline of Crime Prevention: A Systematic Approach to its Nature, Range and Concepts' in Bennett T (ed) *Prevention Crime and Disorder: Targeting Strategies and Responsibilities*, Cambridge: Institute of Criminology.

Eklom, P (2000) 'The Conjunction of Criminal Opportunity, A tool for clear, 'joined-up' thinking about community safety and crime reduction', in *Secure Foundation, Key Issues in Crime Prevention, Crime Reduction and Community Safety*, London: IPPR.

Electronic Privacy Information Centre (1997) 'Surfer Beware: Personal Privacy and the Internet,' June 1997, <http://www.epic.org/reports/surfer-beware.html>

Felson, M (1987) 'Crime and everyday life', Thousand Oaks, California: Pine Forge Press.

Giddens, A (1990) 'The Consequences of Modernity', Cambridge: Polity Press and Beck, U (1992) *Risk Society* London: Sage.

Kleinig, J (2000) 'The Burdens of Situational Crime Prevention' in Von Hirsh, A, Garland, D and Wakefield, A (eds) *Ethical and Social Perspectives on Situational Crime Prevention*, London: Hart.

Palmer, G (2000) 'The New Spectacle of Crime,' in Thomas, D and Loader, B.D (eds) *Cybercrime Law Enforcement, Security And Surveillance In The Information Age*, London: Routledge.

Von Hirsch (2000) 'The Ethics of Public Television Surveillance' in Von Hirsh, A, Garland, D and Wakefield, A (eds) *Ethical and Social Perspectives on Situational Crime Prevention*, London: Hart.