

Identity Theft in a Social Context: Paper presented to Digital Identity Forum

November 2nd 2006

**Dr Yvonne Jewkes, Reader in Criminology, International Centre for Comparative
Criminological Research, Open University, UK**

New ways of committing old crimes

One of the themes of *Dot.cons Crime, Deviance and Identity on the Internet* concerns how, in cyberspace, identity is not fixed but is an ephemeral, fluid entity open to constant renegotiation, change and manipulation. In the Introduction to that book I write that there is a blurred line between 'playful' and fraudulent, inclusive and exploitative, accessible and extremist, 'deviant' and criminal. The Internet affords its users freedom of speech, freedom of access, freedom of information, freedom to join subcultures and fan cultures, even freedom to hide, change or play with one's identity. At the same time, it facilitates an unprecedented level of anonymity, is difficult to police, and is virtually impossible to censor. It is for these reasons that a series of local and global moral panics about the Internet have been generated in the last decade (for overviews see Jewkes, 2003; 2007).

Of course, there is nothing inherently sinister in the technology itself. Like wider debates about the effects of harmful media content, much public discussion about computer-related crime is underpinned by a strong technological determinism (that is, overstating the power of the technology and underplaying the importance of the individual actor). But most cybercrimes are reasonably common offences, and computer technologies have largely provided a new means to commit 'old' crimes. The most that can be said with any degree of certainty, then, is that individuals who might otherwise have been predisposed to commit suicide, murder, abduction, fraud and theft might be drawn to the Internet to facilitate their desires, particularly if their behaviour receives support from communities of other people who are sympathetic to their thoughts, values and behaviour.

What makes the role of the Internet unique, and mitigates against the argument that criminal and anti-social activities on the Internet are analogous to similar behaviour in the physical world, is its scale and reach. It took the World Wide Web just three years to reach its first 50 million users; a feat which eluded

television for 15 years and which took radio 37 years to achieve from its point of inception (Naughton, 1999). A mere decade after it became a domestic, as opposed to military, technology, the number of Internet users was estimated at around 1 billion and, in the UK, a recent study on behalf of Google found that Internet use has overtaken television as the chief non-work activity (apart from sleeping) with the average user spending around 164 minutes online every day, compared with 148 minutes watching television (*Guardian*, 8th March 2006).

While much of the debate about Internet regulation and censorship appears to be based on speculative notions of the extreme anti-social and harmful impacts it may have at some point in the future¹ it is the more mundane crimes of identity theft and identity fraud that dominate public concerns and anxieties. The British government estimates that identity fraud cost the UK £1.7bn in 2005, and has risen more than five-fold since 1999 (from 20,000 cases to 137,000 cases). A study carried out by the US Department of Justice found that about 3 *per cent* of American households (approximately 3.6 million) were victims of identity theft in a six-month period in 2004. The most common offence involved unauthorized use of credit cards and the average loss was \$1,290 (www.ojp.usdoj.gov/bjs).

Towards a surveillance society

One of the solutions proffered to combat identity fraud and theft is a move away from token-based or knowledge-based systems to the accumulation of coded information from genetic material biometrics. In the global surveillance society one is no longer identified by what one has (e.g. a passport or credit card), or by what one knows (e.g. a PIN), but increasingly by what one *is* – a collection of unique body parts (Lyon, 2001). Advances in technology - leading to initiatives as diverse as store loyalty cards; identity cards; DNA databases; electronic ‘tagging’ of offenders (and of newborn babies in hospitals and, in some cases school-aged children by worried

¹ Such predictions of apocalyptic meltdown include terrorist acts intended to sabotage water, gas and electricity supplies, close all international communications, manipulate air traffic control or military systems, hack into a hospital’s computer system and alter details of medical conditions and treatments, tamper with National Insurance numbers or tax codes, and paralyse financial systems. However, most commentators believe that while these kinds of possibilities are terrifying to contemplate, the likelihood of such calamitous events occurring through human or software error is far greater than the chance of malicious hackers, mercenaries or terrorists bringing down a country’s infrastructure and, for the time being at least, they remain hypothetical possibilities rather than perpetrated acts of aggression (Jewkes, 2003).

parents); voice recognition; hand geometry; iris and retina scans in environments as diverse as workplaces, airports, border controls and refugee centres, and so on - have arguably expanded the 'disciplinary gaze' beyond the confines of the prison and the factory, to encompass the community as a whole. Social control is extended beyond individuals and discrete groups to entire populations, creating a 'carceral society' (Foucault, 1977).

The questions thus arise; is surveillance evenly distributed and does it impact on some people negatively and others positively? Much criminological discussion is concerned with the ways in which surveillance systems are bound up with wider relations of power and discipline, reinforcing existing inequalities along traditional lines of class, gender, ethnicity, economic status and age, and many criminologists are sceptical (if not downright hostile) to the idea that biometric technologies liberate and empower the general citizenry, far less protect them from crime, terrorist attacks, and other forms of victimization. Some commentators argue that politicians, the media and the criminal justice system set the agenda for public debate about crime and the implementation of criminal justice, and collude in perpetuating notions of 'enemies within'. These agendas then shape public perceptions, not only about their likelihood of being a victim of crime, but also about who they should fear. Consequently, criminal justice is determined by very narrow legal definitions that ignore, tolerate, accept, or even applaud the crimes of the powerful, while criminalising the disadvantaged and perpetuating social exclusion.

Biological tokens of identification are offered as a vital defence in identifying individuals with spoiled identities - and even whole undesirable populations - in the new global order. Through the use of biometric ID cards, the practices of identifying the 'other' are proliferating and have the potential to be built into a number of automated bureaucratic systems, such as welfare and medical aid. For example, Katja Franko Aas (2006) notes that in 2002, in the mountainous border crossings between Afghanistan and Pakistan, the United Nations High Commissioner for Refugees set up several iris scanning machines in an attempt to eliminate fraud and to be more accountable to their donors. The scanners took photographs of eyes of tens of thousands of Afghan refugees, children and adults, in order to determine whether they were eligible for humanitarian aid. The photos were then converted into digital code and stored in a database. If a refugee, who had already received help, returned for more, he or she was automatically recognised by the database and

denied. At the same time, biometrics is used at borders and airports to speed up the travel of low risk populations through various fast-track initiatives for frequent flyers. In a time of heightened insecurity about global mobility, then, surveillance of the body serves as a form of 'social sorting' distinguishing between low and high risk populations - or between 'us' and 'them'. Surveillance of the body is thus moving from a practice exercised over marginalized groups such as prisoners and asylum seekers to one that has the potential to affect all of us who work, drive, travel, go to clubs etc. As a result, the experience of being checked as an outsider is no longer reserved only for border crossings, rather, the border is everywhere (Lyon, 2001; cf. Aas, 2006).

Furthermore, while biometric systems are able to give 'scientific' - and therefore indisputable - data about an individual's identity, they are not able to evaluate the credibility of their stories. Profound questions of human nature, character evaluation, risk, danger and trustworthiness are turned into simple, empirical questions of false and positive that can be answered by technology (Aas, 2006). In other words, biometrics gives us information but it doesn't give us knowledge about people and the causes of their actions; it is information based on one-way observation rather than knowledge learned from mutual communication. It is, moreover, information marked by power relations: 'The decision about denial of entry into a country can be reached almost entirely by a technological system, rather than having to address the intricate issues of need, despair and justifications for help' (Aas, 2006: 146).

Biometric identification can, therefore, not only serve as a point of discussion of the importance of the body and personal/social/legal identity in contemporary culture, but also as an image of the changing mechanisms of social exclusion. The media's construction of crime and violence as random and unpredictable arguably not only encourages people to retreat into their private domains behind locked doors, gated communities, the bull-bars of their SUVs, and virtual identities, as a means of managing their everyday personal risk, but also encourages them to accept increasingly repressive forms of social control in the public sphere. Arguably, most citizens have come to take for granted that they are observed, monitored, classified and controlled in almost every aspect of their public lives. Most of us barely notice the extent to which we are at the centre of a surveillance society, so easily have we internalised the changes in our conduct (using swipe cards instead of keys to access

our workplaces, banking by telephone or computer rather than 'in person, and so on). If one wishes to take advantage of credit, withdraw money from a bank, work for an employer, vote in an election, purchase goods, attend a football match, drive a car, catch a train, use a mobile phone or surf the Internet, it is virtually impossible to remain anonymous. Quite simply, recent years have witnessed the 'disappearance of disappearance' (Haggerty and Ericson, 2000).

Who watches the watchers?

The theoretical implications of these social phenomena point to the fact that not only do surveillance systems underpin correctional policies, but that they have created a new mode of governance. The 'rehabilitative ideal' with its promise of 'treating' the sickness that causes individuals to offend, and its evocation of a benevolent state concerned to eradicate poverty, deprivation and hardship, dominated criminological discourse throughout much of the twentieth century. But in recent years, as public concerns about crime and the perceived failures of the criminal justice system have intensified, those in power have retreated from any pretence of liberalism and adopted the language of authoritarian populism, using phrases like 'prison works', 'zero tolerance' and 'tough on crime'. While one objective is to develop methods of situational crime control, a related aim is to single out those who do not 'belong' in these environments, and take pre-emptive action to exclude them. Thus, rather than attempting to tolerate, understand and rehabilitate the different and the dangerous, there has been an ideological shift towards the less expensive and simpler task of displacing them from particular locations and from opportunities to obtain goods and services; of restricting mobility and behaviour; and of managing them rather than changing them. These shifting attitudes are increasingly being seen not simply as attempts to govern crime but also to involve 'government through crime'; a new 'governmentality' (Stenson, 2001).

Government of crime is thus practised, not only by police and criminal justice professionals, but also by the insurance industry, communities, employers, retail managers and so on (O'Malley, 2001). Often justified in terms of their ability to monitor 'risk' groups who pose a significant threat to economic stability or social order, the surveillance measures adopted by these diverse bodies can quickly lead to much broader definitions of criminalisation and dangerousness being adopted. One example is the establishment of a UK National DNA Database, originally set up to

aid the identification of serious violent and sexual offenders but now containing DNA samples taken without consent from any person convicted or *suspected* of a recordable offence at the point of arrest, even if subsequently acquitted.

It is issues such as these that cause many commentators to question whether biometrics are privacy-enhancing or in fact invade privacy; whether they empower citizens or empower the state (of course, the answer is both). Some of the main privacy fears include concerns that biometric information will be gathered without permission or knowledge, or without explicitly defining the purpose for which it is required; that information may be used for a variety of purposes other than those for which it was originally acquired ('function creep'); shared without explicit permission; or used to track people across multiple databases to amalgamate information for the purpose of surveillance or social control (Smith, 2007). Depth of information is further enhanced via the connection of technologies with institutions, creating a coalescence of once discrete systems. Increasingly, in any major crime investigation fragments of data will be coalesced and both the victim and the suspect will have their movements, consumption patterns, reading tastes, personal contacts, sexual histories and various other aspects of their private lives compiled into a detailed file that chronicles their deviation from the 'norm'. For example, following the police hunt for 12-year-old Shevaun Pennington who disappeared with a 31-year-old American in July 2003 after 'meeting' him in an Internet chat room, it was revealed that, despite her family's pleas for information about their missing child and her abductor, the police had known their whereabouts all along, thanks to a GPS (Global Positioning Satellite) system that could pick up the suspect's mobile phone transmissions. Not only did this allow the police to triangulate the phone's location to within a few metres, but they were reportedly able to activate the phone even when it was switched off. In addition, the police alerted credit card companies so that an alarm was automatically triggered when the suspect used his credit card to buy airline tickets. Meanwhile, police examined his personal computer where they found downloaded child pornography, and his victim's computer where it was discovered that, unbeknown to her parents, she had been in communication with the American for over a year.

This example demonstrates that surveillance is far from a unitary technology. It happens to be a high-profile criminal case but even when we consider the mundane monitoring of 'ordinary' citizens, we are in fact referring to a nexus of

cameras, computers, databases, telecommunications, people and, increasingly legal statutes which support the undermining of personal privacy even when done in violation of civil liberties. While joined-up agencies inarguably aid horizontal flows of communication, they operate almost universally through vertical structures of power, often with few or no mechanisms of accountability.

This bleak assessment has become of increased salience since 9/11. One of the developments causing concern to civil liberties groups in the aftermath of the attacks on the World Trade Center and the Pentagon is the passing of the USA PATRIOT Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism). A 342-page document which many in Congress profess not to have read, the Act gives federal officials greater authority to track and intercept communications both for law enforcement and foreign intelligence-gathering purposes. Its critics claim it creates new crimes, new penalties and new procedures for use against American and non-American citizens. Under the guise of fighting terrorists, some believe that the primary purpose of Patriot is to perpetuate public fear within an atmosphere in which anything other than staunch support for the 'war on terror' is considered unpatriotic and dangerous. The provisions made in the Act are esoteric and wide-ranging: among other things, it requires DNA samples of convicted terrorists to be held on a database of 'violent convicts', gives the FBI powers to covertly obtain the transaction records for bookshops and libraries, Internet Service Providers, telephone companies, casinos, travel agents and car dealers, and extends the 'foreign student monitoring program' to include flying, language and vocational schools. And if the fear that prosecution could await anyone who uses the Internet to satisfy their curiosity at to what the *The Anarchists Cookbook* might be seems farfetched, consider the fact that, according to a University of Illinois survey, in Detroit – home to a large Muslim community – some children have stopped taking out books on Islam (<http://news.bbc.co.uk>). Although the Act has met with opposition from communities and legal officials, with some US District Courts ruling sections of it unlawful, fears remain that the US government will continue to award itself powers to investigate an even greater spectrum of nationals and non-nationals alike without probable cause and beneath a veil of secrecy.

There is little doubt that surveillance technologies have radically destabilised the public/private boundary. Yet it is frequently claimed that, in the wake of 9/11, the climate of political and public acceptability has become more favourable to the

idea of surveillance. For example, many governments are trying to gain public support for mandatory 'smart' ID cards that can hold a wide range of coded data, and could incorporate national identity card, driver's licence, health details, passport information and e-cash applications as well as eye scans or thumbprints. In the UK, as elsewhere, identity cards are presented by government as a panacea to the problems of illegal immigration, crime and terrorism. But many criminologists and cultural commentators remain deeply apprehensive about the seemingly relentless drive by governments to oversee and regulate the activities of their citizens and, although surveillance has many and varied (and indeed benign) applications, it is state surveillance that remains of greatest concern. While current fears about terrorism may have mollified the general public into accepting a greater degree of surveillance (and there is no convincing evidence that this is the case), many political commentators, human rights campaigners and civil liberties organisations have expressed extreme disquiet about the licence that governments take in unstable times.

References

Aas, K. F. (2007) 'Beyond "the Desert of the Real": Crime Control in a Virtual(ised) Reality' in Y. Jewkes (ed.) *Crime Online*, Cullompton: Willan

Aas, K. F. (2006) "'The Body Does Not Lie: Identity, Risk and Trust in Technoculture' in *Crime, Media, Culture: An International Journal* 2(2): 143-158

Foucault, M. (1977) *Discipline and Punish*, London: Allen Lane

Haggerty, K. D. and Ericson, R. V. (2000) 'The surveillant assemblage', in *British Journal of Sociology*, 51 (4) December 2000: 605-622

Jewkes, Y. (ed.) (2007) *Crime Online*, Cullompton: Willan

Jewkes, Y. (2003) *Dot.cons: Crime, Deviance and Identity on the Internet*, Cullompton: Willan

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

Naughton, J. (1999) *A Brief History of the Future: the Origins of the Internet*, London: Phoenix

O'Malley, P. (2001) 'Governmentality' in E. McLaughlin & J. Muncie (eds.) *The Sage Dictionary of Criminology*, London: Sage

Smith, R. G. (2007) 'Biometric Solutions to Identity-related Cybercrime' in Y. Jewkes (ed.) *Crime Online*, Cullompton: Willan

Stenson, K. (2001) 'The new politics of crime control' in K. Stenson & R. R. Sullivan (eds.) *Crime, Risk and Justice: the Politics of Crime Control in Liberal Democracies*, Cullompton: Willan