International Review of Law, Computers & Technology
Vol. 24, No. 3, November 2010, 299–308

Tough on data misuse, tough on the causes of data misuse: A review of New Labour's approach to information security and regulating the misuse of digital information (1997–2010)

Jonathan Bishop*

Centre for Research into Online Communities and E-Learning Systems, Glamorgan Blended Learning Ltd, Abercynon, Wales, UK

New Labour was a description of a particular approach to government of the British Labour Party, which was in power in the United Kingdom between 1997 and 2010. While this government initially envisaged an end to the social causes of misdemeanours, its actions led to a greater number of laws on the statute books creating thousands of statutory offences. A small number of these had direct effects on the number of computer related offences that were able to be prosecuted. This paper reviews these laws, and the role of legal systems in responding to the increasing number of misdemeanours that are occurring in computer environments for which New Labour's approach of creating more statutory offences has not addressed.

Keywords: computer law; conflict; resolution

Introduction

Tony Blair said that New Labour, the name for the 'third way' version of the British Labour Party, which came about through his reforms, would be 'tough on crime and tough on the causes of crime'.[1] This tactic that saw him triangulate into an area of policy normally held by the Conservative Party, and led to the Labour Party winning a landslide victory in the UK general election of 1997.[2] According to Calcutt,[3] New Labour exemplified the end of the old state and, in turn, New Labour's connection to the Internet exemplified the party's newness and its abandonment of out-of-date labour movement traditions. However, in 2008, 11 years after the dawn of New Labour, thousands of new offences had been created.[4] While not authoritative sources, the British newspaper *The Telegraph* reported in 2008 that the New Labour Government had introduced 3600 new offences since 1997, the year they came to power, and by 2010, the year they left power, this had risen to 4300 according to the populist British tabloid newspaper, *The Sun*. This suggested that New Labour represented state-control more so than was envisaged in 1997, although it could be argued that this was New Labour's way of enshrining their party's commitment to ensuring the rights that the people in society enjoy should reflect the duties they owe. However, it may also be argued that creating more criminals is not a way to create a society based on equality of opportunity, as it is more likely that vulnerable groups will be on the wrong end of the law as compared to those with power and wealth, as Waiton

*Email: jonathan@jonathanbishop.com

ISSN 1360-0869 print/ISSN 1364-6885 online

DOI: 10.1080/13600869.2010.522336
http://www.informaworld.com

suggests.[5] This outcome of a more criminalised society, after 13 years of New Labour, starkly resembles their early mission to correct the failings of a state that saw prison as something that should be the sentence of first resort.[6] The New Labour philosophy to the contrary, which suggests that misdemeanours have a social cause that should be addressed by the social and criminal justice systems of the state, has not had great attention. The few legislative measures to this effect have been ones such as those that give the authorities greater powers to tackle anti-social behaviour through the legal system.

Whether New Labour has simply been a trend follower as opposed to a trend setter in data misuse legislation is matter of debate. In heavily information-dependent fields such as education, it has been argued that the New Labour government simply mirrored the US government's policy.[7] The anti-terror and extradition policy of the UK was particularly in tune with the USA and Australia after the 9/11 atrocities, and these partners' attitudes to the Internet were also regarded as similar.[8] Despite this, distinct differences appeared to emerge under the leadership of New Labour between Tony Blair's 'shoulder to shoulder' relationship with the USA and Gordon Brown's 'progressive consensus' with the world, particularly during the financial crisis that occurred during Brown's term as a result of the collapse in the US housing market.

A review of data misuse legislation under New Labour

New Labour's policy on the information superhighway in 1995 underscored its faith in education as the prime means for successful accommodation to the demands of a global economy in preparation for it coming to office in 1997.[9] While the early stages of New Labour involved a drive towards educational computing and the Internet as part of their education policy agenda,[10] a raft of new laws creating new offences relating to computer use and misuse subsequently came on to the statute books. New Labour's drive to control technology and information was apparent during its ascension to power, when for example it used a system called 'Excalibur', a database of newspaper and television news stories, to mount instant counter-attacks on Conservative Party criticisms,[11] something which is now in effect available to all through Google's news archives and academics and other professionals to a greater extent through the Nexis database.

Information security and privacy

One of New Labour's first pieces of legislation relating to computers was the Data Protection Act 1998 (DPA). This acts purpose was to 'make new provision for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information'.

The Act introduces new offences in respect of processing data illegally and failing to adhere to notification regulations. According to Cannataci and Bonnici,[12] whereas the New Labour government did fulfil its electoral promise and bring about the enactment of the long overdue Human Rights Act, it failed to do the logical thing and treat data protection as being a rightful heir of the same standing. However, others have argued that even in the form it took, the DPA has led to significant changes in the way personal data are collected and stored by researchers and data intensive groups, which is protecting some of the more vulnerable people in society.[13] However this extra protection has not been welcomed by all as Gilkes et al.,[14] for instance, consider these protections of data to be bureaucratic. Tranberg and Rashbass[15] have also mentioned the concern of health professionals towards the DPA, who argue that it is inappropriate for dealing with the particular considerations relevant to

health information, because it was written principally for the financial and commercial sectors. The extent of the DPA's reach is only just becoming apparent. In *Common Services Agency* v. *Scottish Information Commissioner* [2008] UKHL 47, it was clarified that while the word 'data' is defined in Section1(1) of the act, the word 'information' is not. The Court ruled that for the purposes of the 1998 Act, 'data' means information which is in a form capable of being processed by a computer or other automatic equipment, or is recorded with the intent that it be should be processed by such means, as well as that which is recorded in file systems. Cases like this in the UK have generally involved the discussion of definitions of various aspects, due to the law mainly being interpreted literally, rather than proportionally as is the case in many other jurisdictions in the European Union (EU). While the Court of Appeal in *R (on the application of Wood)* v. *Metropolitan Police Commissioner* [2009] EWCA Civ 414 did not comment on how the DPA affects photography, according to Clarka, Prosserb and Wilesc[16] the DPA does affect researchers' use of photography, including its use in public spaces. They point out that a digital image of an individual can be considered to be personal data for the purpose of the Act, and therefore requires consent.

New Labour said in a 1995 policy document when they were in opposition that 'attempts to control the use of encryption technology are wrong in principle, unworkable in practice, and damaging to the long-term economic value of the information networks'. Despite this, they introduced the Electronic Communications Act 2000 (ECA), which had as its provisions to 'facilitate the use of electronic communications and electronic data storage', and to 'make provision about the modification of licences granted under Section 7 of the Telecommunications Act 1984; and for connected purposes'. The first part of the Electronic Communications Act 2000, better-known for granting legal status to electronic signatures, gave the government the ability to introduce 'a register of approved providers of cryptography support services'.[17] It also introduced an offence where information gained under the Act was disclosed. The ECA allows for the use of an electronic signature where traditionally a written signature was required, with restrictions on what is acceptable.[18]

Many cases around the ECA have been whether something constitutes a signature within the meaning of the Act. In *J Pereira Fernandes SA* v. *Mehta* [2006] EWHC 813 (Ch) Judge Pelling ruled that if a party or a party's agent sending an e-mail types his or her or his or her principal's name to the extent required or permitted by existing case law in the body of an e-mail, then in his view that would be a sufficient signature for the purposes of Section 4 of the ECA. The ECA does not, however, tackle the problem of identifying those on the Internet who carry out misdemeanours on an anonymous basis.[19] This lack of a requirement that Internet users electronically sign their Internet contributions means that provisions in another of New Labour's pieces of legislation, the Regulation of Investigatory Powers Act 2000 (RIPA), are needed.

Crime prevention and detection

New Labour introduced a number of pieces of legislation to detect and combat computer related crime, some of which were very contentious. RIPA had as its purpose to:

> make provision for and about the interception of communications, the acquisition and disclosure of data relating to communications, the carrying out of surveillance, the use of covert human intelligence sources and the acquisition of the means by which electronic data protected by encryption or passwords may be decrypted or accessed; to provide for Commissioners and a tribunal with functions and jurisdiction in relation to those matters, to entries on and

> interferences with property or with wireless telegraphy and to the carrying out of their functions by the Security Service, the Secret Intelligence Service and the Government Communications Headquarters; and for connected purposes.

RIPA introduced statutory offences of failing to disclose information demanded by a notice issued under the Act and disclosing the information requested in the notice to a party not named in the notice. RIPA has led to increased access to and sharing of public and private sector data through gateway agreements and other areas.[20] This Act was not entirely well received, with some academics questioning the approach of the government and whether it was appropriate in a liberal democracy.[21] In *Kennedy* v. *United Kingdom* [2010] All ER (D) 224, the European Court of Human Rights ruled that while the surveillance measures permitted by RIPA had pursued the legitimate aims of the protection of national security, the prevention of crime and the protection of the economic well-being of the country, it had to be determined whether the procedures for supervising the ordering and implementation of the restrictive measures were such as to keep the 'interference' to what was 'necessary in a democratic society'.

The Fraud Act 2006 (FA) had as its purpose to 'make provision for, and in connection with, criminal liability for fraud and obtaining services dishonestly'. The Act has wide application to data misuse and is more likely to be used by the judiciary in place of the Computer Misuse Act 1990 (CMA) due to its apparent clarity.[22] The FA has wide provisions on requiring those in positions of authority where they have responsibility for protecting the financial interests of others to not abuse this position. This could cover information technology (IT) projects where a contractor may be willing to take unnecessary risk, or even where a project manager claims expenses against a job that benefits them personally and are not essential to the project. The practice of forging cookies is now also more likely to be prosecuted under the FA as opposed to the CMA.[23]

Telephony, wireless and television related legislation

The Mobile Telephones (Re-Programming) Act 2002 had as its purpose to 'create offences in respect of unique electronic equipment identifiers of mobile wireless communications devices'. It made it an offence if a person to change a mobile phone's unique device identifier, such as the subscriber identity module (SIM) card, interfere with a unique device identifier's operation, offer or agree to re-programme a mobile telephone, or to offer or agree to another person reprogramming a mobile telephone.

The Television Licences (Disclosure of Information) Act 2000 (TLA) had as its purpose to 'make provision about the disclosure of certain information for purposes connected with television licences'. It introduced new offences relating to disclosure of information gained under the Act, as with the ECA. The Digital Switchover (Disclosure of Information) Act 2007 (DSA) has as its purpose to 'make provision about the disclosure of certain information for purposes connected with digital switchover'. The Act, like the ECA and TLA, introduced offences for disclosing information obtained under it. Both these Acts served to give specific bodies the opportunity to implement New Labour's social inclusion agenda, which started with their implementation of the New Deal Programme.[24]

The Communications Act 2003 had as its purpose to

> confer functions on the Office of Communications; to make provision about the regulation of the provision of electronic communications networks and services and of the use of the electromagnetic spectrum; to make provision about the regulation of broadcasting and of the provision of television and radio services; to make provision about mergers involving newspaper and

> other media enterprises and, in that connection, to amend the Enterprise Act 2002; and for connected purposes.

The Act introduced new offences for 'Improper use of public electronic communications network', 'dishonestly obtaining electronic communications services' (Section 125), 'possession or supply of apparatus etc. for contravening' (Section 126) and 'improper use of public electronic communications network', among other information disclosure offences.

The Crown Prosecution Service considers that the Section 125 charge of the CA may be more appropriate than one of obtaining services dishonestly contrary to Section 11 Fraud Act 2006; or a Section 1 Computer Misuse Act 1990 unauthorised access offence where access to a telecoms service was obtained without permission. Section 126 has opened anyone in possession of a device such as a Wi-Fi detector to the charge of possessing apparatus for contravening Section 125 should the authorities choose to act. For someone to be prosecuted under the Act for sending an improper message, according to *DPP* v. *Collins* [2006] 1 WLR 2223 the message needs to cause 'gross offence' to those to whom it relates who need not be the recipients. In that particular case, it was held that a message relating to ethnic minorities need not to have been sent to them directly in order for a conviction under the Act to be made if the message about them was grossly offensive.

The Wireless Telegraphy Act 2006 (WTA) had as its purpose to 'consolidate enactments about wireless telegraphy'. The WTA was successful as cited in *Office of Communications and another* v. *Floe Telecom Ltd* [2009] EWCA Civ 47 to show that in the absence of a licence or exemption granted or made under Section 8 of the Act, the use of Global System for Mobile Communications (GSM) gateways (including Commercial Multi-User Gateways) for the purpose of providing a telecommunications service by way of business to another person is unlawful.

Despite being a consolatory Act, Section 48 of it introduced a new offence of 'interception and disclosure of messages'. The Crown Prosecution Service indicates that using this legislation the prosecution must prove utilisation or employment of the apparatus over and above mere possession and that acquiring evidence of the suspect switching on or tuning to unauthorised frequencies' will assist in proving utilisation.

Equality and human rights legislation

The Human Rights Act 1998 (HRA) had as its purpose to:

> give further effect to rights and freedoms guaranteed under the European Convention on Human Rights; to make provision with respect to holders of certain judicial offices who become judges of the European Court of Human Rights; and for connected purposes.

The HRA gave legitimacy to UK legislation relating to defamation, where it became a requirement for the government to protect the reputation of citizens when regulating freedom of expression. Since 1998, the impact of the Human Rights Act has reached far beyond constitutional matters, into statutory interpretation, counter-terrorism legislation, general criminal law and the horizontal effect of rights in private law disputes.[25] The Act also opened up a number of potential points of conflict with regard to the rights of people to use the Internet and online communities that are part of it. For instance it gives effect to Article 11 of the convention, which while not being interpreted as imposing an obligation on associations or organisations to admit everyone wishing to join, says people do have a right to apply to join them in order to further the expression of their views and practices as

set out in *Associated Society of Locomotive Engineers & Firemen* v. *United Kingdom* (ECHR, App no 11002/05). An organisation is an undertaking within the meaning of the EU Treaty and the term undertaking has a broad meaning in EU Law, which can include someone who hosts a bulletin board. This means that someone should have a human right to be able to apply to join an online community, but they have no right to be a member if the administrators choose not to accept them. The HRA has further opened up difficulties for employers wanting to monitor their employee's emails, because as a result of the Act it is now best practice to have computer usage policies that include the consent of employees for the reading of their e-mails to overcome privacy concerns.[26]

The Equalities Act 2006 (EA) had as its purpose to provide for:

> the establishment of the Commission for Equality and Human Rights; to dissolve the Equal Opportunities Commission, the Commission for Racial Equality and the Disability Rights Commission; to make provision about discrimination on grounds of religion or belief; to enable provision to be made about discrimination on grounds of sexual orientation; to impose duties relating to sex discrimination on persons performing public functions; to amend the Disability Discrimination Act 1995; and for connected purposes.

While not explicitly related to computers, it introduced offences against those who failed to provide goods and services to certain groups on the same grounds they would other members of the public or others in that group. In *Royal Bank of Scotland Group Plc* v. *Allen* [2009] EWCA Civ 1213 it was shown that a bank offering a customer wheelchair Internet banking facilities did not constitute a reasonable adjustment to accessing a bank that had an inaccessible physical location under the Equalities Acts, which could have implications for firms seeing the Internet as a way of overcoming their duties under the Equalities Acts.

The Digital Economy Act

While it may be interesting to compare the approaches in computer misuse legislation between New Labour under Tony Blair, compared to Gordon Brown's administration, the only thing to note is under the latter the approach with regards to computer related legislation followed an exhaustive consultation process, leading to few pieces of legislation. In their final days of government under Gordon Brown, New Labour passed the Digital Economy Act 2010 (DEA), which had as its purpose to

> make provision about the functions of the Office of Communications; to make provision about the online infringement of copyright and about penalties for infringement of copyright and performers' rights; to make provision about internet domain registries; to make provision about the functions of the Channel Four Television Corporation; to make provision about the regulation of television and radio services; to make provision about the regulation of the use of the electromagnetic spectrum; to amend the Video Recordings Act 1984; to make provision about public lending right in relation to electronic publications; and for connected purposes.

The DEA was passed by a late night vote with a result of 189 votes to 47 after a series of compromises and concessions.[27] The most controversial aspect of this legislation was a section to extend the rights of copyright holders so that they can request from an Internet Service Provider (ISP) a list of all the subscribers to that ISP that have infringed their copyright by amending the Communications Act 2003. However, the DEA did not create any new offences in itself, but instead gave the UK's communications regulator, Ofcom, greater powers to enforce copyright on behalf of copyright holders without legal action while giving the offending subscriber the right to appeal against the assumption that they were guilty of an act of copyright theft.

Alternative approaches for tackling computer and data misuse

Whether the DEA is a step towards the 'erosion of human rights' through removing the presumption of innocence by requiring the accused to have to appeal in order to get a 'fair trial' as some have claimed is a matter of debate. It could be argued for instance that this was the first step Gordon Brown took using his 'moral compass' to end the criminalisation of society seen under Tony Blair. Had Gordon Brown formed the next government following the 2010 General Election this may have been the shape of things to come, which may have been a welcomed step away from New Labour's 4300 new offences, towards a society where citizens were made accountable for their actions without being branded a 'criminal'.

Computer scientists have long argued that people do not always know the reason why they carried out a particular action until after the event.[28] They have further argued that the context in which people perceive the actions of themselves and others is unique to them,[29] meaning their interpretation of the circumstances surrounding a misdemeanour, for instance, will be different from that of another. It has also been argued that people in any given context will be limited by their goals within that situation,[30] meaning that in defence of their actions, or while negotiating a contract, they may be limited by how their understanding of the situation has been framed, by them or others.

Contemporary criminal law in the UK usually requires that citizens who have been charged with an offence be proven to have *mens rea* (i.e. 'guilty mind') in some cases, but in all cases they must have *actus reus* (i.e. 'guilty act') in order to secure a conviction. *Mens rea* often means that a citizen is guilty of an offence if they intended to bring about a certain set of consequences, for instance, a hacker who initiated a denial of service attack in order to bring down a website, an action for which there still has not been a successful conviction in the UK under the Computer Misuse Act 1990.

The Internet is fast changing the shape and nature of misdemeanours and computer misuse. As has been demonstrated this is not just through actions online but also as a result of the way technology has impacted on society as a whole. New Labour's approach to introduce offence after offence clearly is not working, as after a reported 4300 new offences the legislation on the statute books has only scratched the surface of the network society that now exists.

Reasonable laws for reasonable people

The UK's House of Commons assumes that all its Members are honourable people. The question that follows therefore is how would the approach to computer misuse change if it was assumed that all people were honourable people and that their misdemeanours, such as computer misuse, are not crimes that need associated offences enshrined in law, but transgressions, which are not typical of the way they would act under perfect conditions. All of the Members of Parliament (MPs) who were shown to have acted improperly in the expenses scandal of the 2005–2010 Parliament were not subject to a penalty under the Theft Act like a citizen would be if they 'obtained a false discount' using a computer system for instance, but instead were given the opportunity to give restitution to the parliamentary authorities. If it is possible for these individuals to be considered to have had lapses of consciousness and not intended to be a criminal or offender, what would be the impact of such a system if granted to all citizens?

If it was assumed that Suchman[31] was correct and that people do not know the full reasons behind their actions until after they have carried out, as was claimed of the MPs who 'acted within the rules', then the requirement for *mens rea* would become dormant, as it would be expected that citizens were not always aware of the consequences of their

actions. This would especially be applicable to computer misuse, where actors are often in a 'state of flow', particularly in online communities,[32] where they are so engaged in the system that they lose consciousness of their actions. The requirements in such a legal system to no longer prove *mens rea*, but to instead only prove *actus reus*, would have impacts on New Labour's legislation with regard to mental capacity. The Mental Capacity Act assumes that everyone has capacity until they otherwise say so or a medical professional does. If people were assumed to be honourable individuals, who because they were human made transgressions, they would only need to declare whether they believe their claimed misdemeanour falls below the standard required by society (i.e. *actus reus*), and not whether they intended or planned the act (i.e. *mens rea*), as is currently allowed of MPs who are referred to the UK Parliament's standards committee.

This could perhaps be considered to be an extension of New Labour's Protection from Harassment Act, which stipulated that any repeated form of conduct against someone could be deemed a crime,[33] and its Antisocial Behaviour Act, which led to people being issued with injunction-like notices by a court, called Anti-Social Behaviour Orders, which prescribed that if they carried out a particular act that others objected to then they would face a prison sentence. In such a legal system, the flexible nature of Common Law would have to mean that it would only be necessary for a judge and/or jury to rule whether a person (1) carried out the particular act and (2) whether they were reasonable in their actions, based on the definition set out by Lord Devlin in reference to the 'man on the Clapham omnibus'. This definition is variable depending on the age, experience and qualifications of the accused in relation to the act they have been proven to have carried out. So for example, it may be reasonable to expect an IT Manager to understand the policies of their organisation and professional body in relation to sending inflammatory messages, known as 'flames', for instance, but it may not be expected that a child would be reasonably expected to understand the consequences of their actions using a computer in their school. In this case, the judge would adjust the severity of any sentence based on the consensus of the jury, which may form a persuasive precedent where appropriate.

It should also be questioned that if everyone is assumed to be as honourable as an MP, whether there is a need for the criminal courts to have jurisdiction over all misdemeanours, or whether tribunals where the consequences are more understandable to the accused and the court may be appropriate, as happens with the Parliamentary Standards Committee in the case of MPs. Misdemeanours of children may be more appropriately dealt with outside of the courts for instance, and in the UK, the malpractice of a medical doctor may be more appropriately handled by the British Medical Association (BMA) than the Crown Court. If brought before the court, the accused may not have a jury of their actual peers presiding over their case, whom have a more complete understanding of their profession and what is reasonably expected. If every working person was required to be a member of a professional body, which could reduce the level of responsibility and therefore earning potential if they acted in a way that was not reasonable, then there may be a greater degree of dissonance when they are engaged in the use of computer systems, for instance. An IT Manager may be less willing to send a flame for instance if they thought that the BCS, which is the Chartered Institute for IT in the UK, would reduce the grade they could work at to that of a technician. A legal system such as this would be based on an ethical code rather than a criminal code, so it would not be necessary, as New Labour has done, to specify under every Act allowing the use of information and offence for disclosing it, as it would be expected by most professions that a reasonable person would not do that and it would be unethical if they did.

Treating all citizens on par with MPs, who can be reprimanded by the parliamentary authorities outside of the legal system if they have acted questionably, and the highly regulated medical professional, where medical doctors can be brought before the BMA if they fall below the standard expected of them, may require a change in the law if it is to be done through public tribunals. At present in the UK, the principle of *casus omissus* states that the judiciary has no right to fill in the gaps in the law where an offence is not defined in statute or common law as set out by Lord Parker in *Fisher* v. *Bell* [1961] QB 394, 400.

Discussion

New Labour was a description of a particular approach to government of the British Labour Party, which was in power in the UK between 1997 and 2010. While this government initially envisaged an end to the social causes of misdemeanours, its actions led to a greater number of laws on the statute books creating thousands of statutory offences. A small number of these had direct effects on the number of computer related offences that were able to be prosecuted. A various number of Acts of Parliament relating to computers created offences of disclosing information received under them, such as the Electronic Communications Act 2000, the Televisions Licensing Act 2000 and the Digital Switchover Act 2007, among others. The Data Protection Act 1998 was one of New Labour's first pieces of computer related law, which it was argued failed to do the 'logical thing' and treat data protection as being a rightful heir of the same standing to the Human Rights Act published the same year. The Digital Economy Act 2010, which was one of New Labour's last pieces of legislation, instead of creating new offences relating to copyright theft, gave copyright holders the opportunity to take non-criminalising action against those that abused their rights. This Act, which the new government of 2010 said they will not repeal and which was one of the last pieces of law of New Labour, could be the first step towards 'delegislating' society, so that citizens are held responsible for their actions where they have not acted reasonably, in line with common law precedent, meaning there could be no need to create further offences. This paper questions whether a reformed legal system where the conduct of citizens is more likely to be regulated by professional bodies with the right to reduce the level to which they can practice their profession, is likely to be more effective at tackling computer misuse. Using evidence from computer science literature it was suggested that it may be because it could increase the dissonance that citizens experience before they carry out an act that a reasonable person would not, while accepting the assumption of Lucy Suchman that individuals are not always aware of why they did something until after the event. Concerns over the limitations of the Electronic Communications Act 2000 in not requiring people to verify their identity online may need to be addressed if the concerns over the 'snooping' powers of the Regulation of Investigatory Powers Act 2000 are to be addressed.

Notes

1. S. Charman and S.P. Savage, 'The New Politics of Law and Order: Labour, Crime and Justice', in *New Labour, New Welfare State? The 'Third Way' in British Social Policy*, ed. M. Powell (London: Polity Press, 1999), 191.
2. D. Morris, *Power Plays* (London: Harper Collins, 2002).
3. A. Calcutt, *White Noise: An A–Z of the Contradictions in Cyberculture* (Basingstoke, UK: Palgrave MacMillan, 1999).
4. S. Waiton, 'Policing After the Crisis: Crime, Safety and the Vulnerable Public', *Punishment & Society* 11, no. 3 (2009): 359.
5. Ibid.

6. N. Lacey, C. Wells and O. Quick, *Reconstructing Criminal Law: Text and Materials* (Cambridge: Cambridge University Press, 2003), 219.
7. G. Wilkinson, 'Commercial Breaks: An Overview of Corporate Opportunities for Commercializing Education in US and English Schools', *London Review of Education* 4, no. 3 (2006): 253–69.
8. K. Gillan and J. Pickerill, 'Transnational Anti-War Activism: Solidarity, Diversity and the Internet in Australia, Britain and the United States after 9/11', *Australian Journal of Political Science* 43, no. 1 (2008): 59–78.
9. K. Robins, 'Foreclosing on the City? The Bad Idea of Virtual Urbanism', *Technocities*, (1999): 34–59.
10. N. Selwyn and J. Fitz, 'The National Grid for Learning: A Case Study of New Labour Education Policy-Making', *Journal of Education Policy* 16, no. 2 (2001): 127–47.
11. H. Margetts, 'Computerising the Tools of Government', in *Public Administration in an Information Age: A Handbook*, ed. I.T.M. Snellen and W.B.H.J. van de Donk (New York: IOS Press, 1998).
12. J.A. Cannataci and J.P.M. Bonnici, 'The UK 2007–2008 Data Protection Fiasco: Moving on from Bad Policy and Bad Law?', *International Review of Law, Computers & Technology* 23, no. 1 (2009): 47–76.
13. E.R. Munro, L. Holmes and H. Ward, 'Researching Vulnerable Groups: Ethical Issues and the Effective Conduct of Research in Local Authorities', *British Journal of Social Work* 35, no. 7 (2005): 1023.
14. C.E. Gilkes, M. Casimiro, A.W. McEvoy, R. MacFarlane and N.D. Kitchen, 'Clinical Databases and Data Protection: Are they Compatible?', *British Journal of Neurosurgery* 17, no. 5 (2003): 426–31.
15. H. Tranberg and J. Rashbass, *Medical Records Use and Abuse* (Oxford: Radcliffe Publishing, 2004).
16. A. Clarka, J. Prosserb and R. Wilesc, 'Ethical Issues in Image-Based Research', *Arts & Health* 2, no. 1 (2010), 81–93.
17. S.A. Mathieson, 'UK Crypto Regulation Option Dies', *Network Security*, no. 6 (2005): 2.
18. L. Reid and M.C. Bromby, 'Beyond Chip and PIN', *Journal of the Law Society of Scotland* 53, no. 7 (2008): 50–1.
19. B. Jayeju-Akinsiku, 'Technology and Electronic Communications Act 2000', *Computers & Security* 21, no. 7 (2002): 624–8.
20. J. Moran, 'Generating More Heat than Light? Debates on Civil Liberties in the UK', *Policing* 1, no. 1 (2007): 80.
21. T. Fitzpatrick, 'Critical Theory, Information Society and Surveillance Technologies', *Information, Communication & Society* 5, no. 3 (2002): 357–78.
22. W.M. Grossman, 'The Charmed Life of Cybercrime', *Infosecurity* 7, no. 1 (2010): 19–21.
23. S. Heron, 'Online Privacy and Browser Security', *Network Security*, no. 6 (2009): 4–7.
24. S. Loo and N. Lucas, 'An Evaluation of the "New Deal" in Further Education Colleges in England', *Journal of Education and Work* 17, no. 3 (2004): 301–13.
25. R. Masterman and I. Leigh, *Making Rights Real: The Human Rights Act in its First Decade* (Oxford: Hart Publishing, 2008).
26. M. Taylor, J. Haggerty and D. Gresty, 'The Legal Aspects of Corporate Computer Usage Policies', *Computer Law & Security Review* 26, no. 1 (2010): 72–6.
27. W.L. Chinese, 'Pressure to Publish Leads to Bias', *Scholarly Communications Report* 14, no. 4 (2010): 7–8.
28. L.A. Suchman, *Plans and Situated Actions: The Problem of Human–Machine Communication* (Cambridge: Cambridge University Press, 1987).
29. G. Mantovani, *New Communication Environments: From Everyday to Virtual* (London: Taylor & Francis, 1996).
30. Ibid.
31. Suchman, *Plans and Situated Actions*.
32. J. Bishop, 'Increasing Participation in Online Communities: A Framework for Human–Computer Interaction', *Computers in Human Behavior* 23, no. 4 (2007): 1881–93.
33. R. Robertson, 'The Increasing Monopolization of Identity by the State: The Case of the UK and the US', *Nationalism and Ethnic Politics* 12, no. 3 (2006): 373–87.