2007

Privacy, Identity and Security

Benjamin J. Goold
Allard School of Law at the University of British Columbia, goold@allard.ubc.ca

Citation Details

Benjamin J Goold, "Privacy, Identity and Security" in Benjamin J Goold & Liora Lazarus, eds, *Security and Human Rights* (Portland: Hart Publishing, [forthcoming in 2007]) 45.

3

PRIVACY, IDENTITY AND SECURITY

Benjamin Goold[*]

> Getting a list in a few seconds of anyone in the United States who subscribes to a Middle Eastern newspaper, watches Al-Jazeera, is between the ages of 20 and 35, and who travelled to Washington on the day of a major political demonstration is but a few clicks away. When a bureaucrat at the TIA (Total Information Awareness) or one of its successors performs such a search and you are named by the state, it is not just 'information' that has been gathered. The e-interpellation goes farther than the information separately considered—by the very act of naming you as a suspect (or 'person of interest') you have changed status in the eyes of others who know about this, and if you come to know or fear, in your eyes as well.
>
> P Galison and M Minow, 'Our Privacy, Ourselves'[1]

In recent years, events such as the attacks of 9/11 and the July 7 London bombings have given rise to major pieces of security legislation in countries like the United Kingdom and the United States. Enacted within months of each other, both the Anti-Terrorism, Crime and Security Act (2001) and the USA PATRIOT Act (2001) contain a range of provisions aimed at increasing the ability of the police, security services and other law enforcement agencies to detect and combat terrorist activities.[2] The

---

[*] I would like to express my thanks to the participants at the Oxford Colloquium on Security and Human Rights for their comments on an earlier version of this chapter, and to Simon Cole, Lisa Gourd, Imogen Goold, Kevin Haggerty, Richard Jones, Simon Halliday, Mike Nellis, and Sophie Walker for their considerable help with subsequent drafts. Any remaining errors or omissions are my own.

[1] Galison, P and Minow, M, 'Our Privacy, Ourselves in the Age of Technological Intrusions' in R Ashby Wilson, *Human Rights in the 'War on Terror'* (Cambridge, Cambridge University Press, 2005) 282–83.

[2] Following a ruling by the House of Lords in *A and others v Secretary of State for the Home Department* [2004] UKHL 56 that the powers contained in Part 4 of the Anti-terrorism, Crime and Security Act (2001) were incompatible with the European Convention on Human Rights, Part 4 was repealed by the Prevention of Terrorism Act (2005). As a result, all measures contained within the Anti-Terrorism, Crime and Security Act (2001) now apply equally to nationals as well as non-

enactment of these Acts, which have been hailed by politicians on both sides of the Atlantic as vital weapons in the 'war on terror', can be directly linked to recent large-scale terrorist events. However, many of the reforms ushered in by these pieces of legislation—although unusually bold and certainly unprecedented in terms of their scope—have largely been in keeping with established trends in the expansion of state power and the decline of privacy in the last years of the twentieth century. In particular, both Acts have led to a marked acceleration in the already rapid growth of existing surveillance networks in the UK and the US. Moreover, the Acts have played a key role in breaking down barriers between various law enforcement agencies, as well as between state and non-state organisations—increasing the ease with which personal information can be exchanged.

Aside from significantly expanding the surveillance capacities of the state and creating new concerns for individual privacy, the Anti-Terrorism and PATRIOT Acts have also weakened longstanding due process protections and the right to a fair trial. This general erosion of the rights of the majority brought about by these and subsequent Acts—though disturbing in and of itself—has been accompanied by a sustained attack on the freedoms of particular minorities, such as Middle Eastern and Muslim communities. Regardless of the intentions of the governments behind them, the provisions contained in these Acts represent a serious retreat from a commitment to human rights in general and a damaging attack on individual privacy in particular.

Privacy is protected as a right—albeit a qualified one—in both the UK and the US, and measures that threaten to undermine individual expectations of privacy must

---

nationals. The USA PATRIOT Act was renewed on 2 March 2006 by both Houses of Congress and subsequently signed into law by President George W Bush on 9 March 2006.

therefore be taken extremely seriously.[3] A great deal has been written about the changing nature of surveillance and the extent to which 9/11 has contributed to the erosion of personal privacy in many Western democracies.[4] However, the aims and provisions of the Anti-terrorism Act and the USA PATRIOT Act should also be seen as significant because they bring to the fore the complex dynamic between security, surveillance, privacy and the construction of identity. The fervour with which security has recently been pursued has not only led to more surveillance and less privacy in the UK and the US, but also contributed to a major shift in the way in which personal identity is constructed and understood by both the state and individual citizens.

In this chapter, the relationship between security, surveillance, privacy and identity will be explored, both in the context of recent legislation such as the Anti-terrorism Act and the PATRIOT Act, and also in the light of ongoing changes in the ways that personal information is gathered, processed and used. In particular, it will be argued that prevailing notions of privacy—and the legal frameworks that aim to protect privacy interests—are ill-suited to defending individuals from an increasingly sophisticated array of surveillance and data processing techniques, which enable information to be acquired and shared at almost zero-cost and which threaten to establish the 'categorical identity' as the primary means by which we are known—to the state and, more disturbingly, to each other.

---

[3] In the United Kingdom, privacy—as defined by art 8 of the European Convention on Human Rights (ECHR)—is protected under the Human Rights Act (1998). In contrast, in the United States privacy derives its status as a right from the First, Forth, Ninth and Fourteenth Amendments to the Constitution. For a discussion of privacy rights in the US, see Alderman, E and Kennedy, C, *The Right to Privacy* (New York, Knopf, 1995); and Goold, B, 'Open to All? Regulating Open Street CCTV and the Case for "Symetrical Surveillance"' (2006) 25(1) *Criminal Justice Ethics* 3–17.

[4] See, for example, Galison and Minow (2005).

REMOVING BARRIERS, REDUCING PRIVACY

Speaking immediately after the signing into law of the USA PATRIOT Act in October 2001, President George W Bush observed that the Act represents a significant step towards the greater integration of law enforcement and security agencies in the United States, in part because it removes many of the barriers to inter-agency communication that existed prior to the events of September 11:

> This legislation gives … intelligence operations and criminal operations the chance to operate not on separate tracks, but to share vital information so necessary to disrupt a terrorist attack before it occurs. As of today, we're changing the laws governing information-sharing.[5]

The issue that Bush was referring to here is known generally in the US as 'linkage blindness'[6] and is now recognised as the major reason behind the failure of the American intelligence services to predict the catastrophic events of September 11.[7] In an effort to address this problem, the PATRIOT Act removed many of the barriers to communication between key agencies such as the Federal Bureau of Investigations (FBI) and the Central Intelligence Agency (CIA), while at the same

---

[5] 'President Signs Anti-terrorism Bill: Remarks by the President at Signing of the PATRIOT Act', The White House, 26 October 2001, quoted by Privacy International, 'Terrorism Profile: US' (3 October 2005), available at http://www.privacyinternational.org (accessed 31 September 2006).

[6] According to Egger, linkage blindness typically arises when organisations fail to recognise areas of mutual interest or jurisdictional overlap and as a consequence duplicate work and refrain from sharing crucial information. See Egger, SA, *Serial Murder: An Elusive Phenomenon* (Westport, CT, Praeger, 1990); and Egger, SA, 'A Working Definition of Serial Murder and the Reduction of Linkage Blindness' (1984) 12 *Journal of Police Science and Administration* 348–57.

[7] In its report to Congress in December 2002, the Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11 echoed earlier concerns about the problem of linkage blindness by stating in its conclusions (84):

> Serious problems in information sharing also persisted, prior to September 11, between the Intelligence Community and non-Intelligence Community agencies. This included other federal agencies as well as state and local authorities. This lack of communication and collaboration deprived those other entities, as well as the Intelligence Community, of access to potentially valuable information in the 'war' against Bin Laden.

A full copy of the report is available at http://www.fas.org/irp/congress/2002_rpt/findings.html (accessed 11 December 2006).

time laying the foundations for the establishment of a new supervisory agency in the form of the Department of Homeland Security.[8] According to section 203(d)(1),

> In general, notwithstanding any other provision of law, it shall be lawful for foreign intelligence or counterintelligence or foreign intelligence information obtained as part of a criminal investigation to be disclosed to any Federal law enforcement, intelligence, protective, immigration, national defense, or national security official in order to assist the official receiving that information in the performance of his official duties. Any Federal official who receives information pursuant to this provision may use that information only as is necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information.

Before the PATRIOT Act, domestic and foreign intelligence gathering and surveillance activities had been deliberately kept separate, in part to ensure the accountability of the various agencies responsible for such tasks and in part to protect civil liberties.[9] These agencies have now been deliberately brought together with clear instructions to intensify their activities and share whatever information they uncover. However, the FBI, CIA, Department for Homeland Security and associated government officials have given little explicit consideration as to how this will affect the second half of the equation—the protection of civil liberties.

Although no equivalent to the Department for Homeland Security has yet been mooted for the United Kingdom, the Anti-Terrorism Act also represents a concerted attempt to improve information gathering and intelligence-sharing by the various agencies that are charged with the task of preventing terrorism and maintaining state security.[10] Prior to the events of September 11, security services such as MI5 and MI6

---

[8] For a detailed discussion of the provisions of the Act, see Doyle, C, 'USA Patriot Act: A Sketch', (Congressional Research Service report RS21203 for Congress, 2005); and Doyle, C, 'USA Patriot Act Sunset: A Sketch' (Congressional Research Service report RS21704 for Congress, 2005).

[9] As Brian Hook observed in his testimony before the House Permanent Select Committee on Intelligence on 9 April 2003, in 1946 President Truman refused to place the CIA under the control of director of the FBI (who, at that time, was J Edgar Hoover) because he feared concentrating so much bureaucratic power in a single individual.

[10] While the current government has yet to argue for the establishment of an equivalent to the US Department of Homeland Security, in a recent speech to Demos, a London think tank, the Home

had never been particularly well-regulated, nor were their interactions with domestic law enforcement agencies formally constrained.[11] As a result, although there may have been concerns in some quarters about the accountability of these agencies and the extent to which Parliament was able effectively to monitor their activities, there were also few significant barriers to inter-agency co-operation and co-ordination.

Nevertheless, with the Anti-terrorism Act the UK government sought to increase the already significant surveillance powers of the state by removing a number of formal restrictions on the use of personal information by the police and immigration services. For example, formerly, section 36 of the Immigration and Asylum Act (1999) required officials to destroy any fingerprints collected during the course of an investigation once that case had been resolved. Section 36 of the Anti-terrorism Act has now removed this requirement. Through an amendment to the Police and Criminal Evidence Act (1984), section 92 of the Anti-terrorism Act also gives the police the power to photograph suspected terrorists regardless of consent.

Significantly, the removal of these restrictions on the use of personal information has coincided with a renewed effort on the part of the government to

---

Secretary John Reid suggested that there was a need for a US-style Minster for Homeland Security. For a report of the speech, see Tempest, M, 'Britain Facing "Most Sustained Threat since WWII" says Reid', *The Guardian*, 9 August 2006, available at http://politics.guardian.co.uk/terrorism/story/0,,1840482,00.html (accessed 31 September 2006).

[11] A major exception to this general trend came with the enactment of the Regulation of Investigatory Powers Act (RIPA) in 2000. In addition to repealing the Interception of Communications Act (1985) (IOCA) and abolishing the post of IOCA Commissioner, RIPA created the position of the Interception of Communications Commissioner and replaced the Commissioners established under the Security Service Act (1989) and the Intelligence Services Act (1994) with a single combined Intelligence Services Commissioner. These two independent Commissioners oversee the activities of the Security Service (MI5) as well as other public bodies charged with protecting national security, such the Secret Intelligence Service (SIS) and the Government Communications Headquarters (GCHQ).

expand the National DNA Database (NDNAD). Established in 1995 by the Forensic Science Service, the NDNAD currently contains over 2 million DNA samples, with some 500,000 new samples being added to the database every year.[12] Although NDNAD is already the largest such database in the world, recent legislation allowing the police to take DNA samples from anyone arrested on suspicion of a recordable offence—again, regardless of consent—is likely to lead to further significant growth in the number of samples held.[13] As the database expands, the use of genetic profiling by the police and other law enforcement agencies, in the context of both domestic crime and terrorism, will also likely increase.[14] Coupled with compulsory identity cards that can be based on some form of biometric identifier, the NDNAD could conceivably provide the basis for a centralised identity register for the entire United Kingdom and could lead to further deliberate co-ordination between immigration and security policy.

Although the FBI's Combined DNA Indexing System (CODIS) contains fewer profiles than the NDNAD (in part because the vast majority of samples are taken from convicted prisoners), the collection of other forms of biometric data, such

---

[12] According to recent Home Office estimates, the NDNAD will hold samples on over 4 million people—approximately 7 per cent of the population—by 2008. This compares with a figure of some 700,000 samples when the current Labour government took office in 1997. See 'Freedom Fears as DNA Database Expands', *The Daily Telegraph,* 5 January 2006.

[13] According to s 10 of the Criminal Justice Act (2003), non-intimate DNA samples can be taken when an individual is in 'police detention in consequence of his arrest for a recordable offence' and provided that a sample of the same type and from the same part of the body has not already been taken (or, if it has been taken, has proved insufficient). For a discussion of the various legal and ethical issues raised by the creation of this database, see Williams, R, Johnson, P and Martin, P, 'Genetic Information and Crime Investigation' (University of Durham School of Applied Social Sciences, report, 2004); and Gene Watch UK, *The Police National DNA Database: Balancing Crime Detection, Human Rights and Privacy* (Buxton, GeneWatch UK, 2005).

[14] McCartney, C 'Forensic DNA Sampling and the England and Wales National DNA Database: A Sceptical Approach' (2004) 12 *Critical Criminology* 157–78.

as fingerprints, has also become a priority for the Department of Homeland Security. At present, almost all non-US nationals are fingerprinted and photographed upon entry into the United States, and there are proposals for such measures to be extended to US citizens as well. The Department of State has explicitly drawn a link between the collection of such data and the successful maintenance of national security:

> The use of these identifiers is an important link in US national security, because fingerprints taken will be compared with similarly collected fingerprints at US ports of entry under the US-VISIT program. This will verify identity to reduce use of stolen and counterfeit visas, and protect against possible use by terrorists or others who might represent a security risk to the US. These two important programs (collecting fingerprints for visa issuance and verifying travelers' fingerprints when they enter the United States) will make travel to the US safer for legitimate travelers, and also improve safety and national security for all Americans.[15]

There may be a danger in drawing too close a comparison between the American and British responses to the events of September 11, yet as the above examples make clear, the two governments have adopted a similar approach to improving state security. In each case, increasing the surveillance powers of the state and encouraging a greater degree of information sharing amongst state institutions have been seen as vital to increasing security and preventing future acts of domestic and international terrorism. Furthermore, both countries are now in the process of establishing comprehensive databases—based, for the moment at least, on the compulsory acquisition of biometric information from non-citizens and criminals. The UK and US governments expect these measures to improve their chances of identifying and apprehending potential terrorists—despite the amorphous nature of the threat and the lack of substantive evidence to suggest that surveillance systems,

[15] For a copy of this statement, see http://travel.state.gov/visa/immigrants/info/info_1336.html (accessed 31 September 2006).

data matching and intelligence-led security measures actually help to prevent large-scale terrorist activities.[16]

In many respects, the fact that both countries have viewed the post-9/11 'security problem' in terms of information is unsurprising. Over the past thirty years the US and UK have grappled with a number of profound social changes—including increasingly diverse populations, increased mobility of citizens and the development of ever more flexible and efficient communications technologies—which have had a particularly significant effect on the ability of the state to provide security for its citizens.[17] These wide-reaching social and technological developments have contributed to a transformation in the nature and purpose of surveillance. Whereas in the past maintaining order and security principally involved the control of physical bodies and the movements of citizens through the use of borders and documentation like passports and visas, the latter part of the twentieth century saw a shift in the provision of security from a static process that was generally fixed in time and space to a dynamic one that is integrated into what Lyon has referred to as 'a world of flows'.[18] Not only can citizens move freely and easily between towns, cities and even countries, but ideas and their more concrete manifestations in literature, images, propaganda, petitions, etc can travel at lightening speeds and reach unimaginably large numbers of people. Maintaining order and security has therefore become an ever

[16] See the contribution by Bernard E Harcourt in this volume.

[17] See Garland, D, *The Culture of Control* (Oxford, Oxford University Press, 2001) ch 4; and Lyon, D, *Surveillance Society: Monitoring Everyday Life* (Buckingham, Open University Press, 2001) ch 6.

[18] Lyon (2001),.

more complex enterprise that relies less on tracking physical bodies than on tracking the data trails that individuals leave behind.[19]

The challenges of securing an increasingly diverse population in an increasingly complex world did not appear out of the blue; but what makes September 11 significant is that it marks the moment at which it became acceptable for governments to draw a direct and very public connection between the demand for security and the need for improved means of general surveillance, individual identification and social control.[20] As Levi and Wall have observed, since September 11 the 'surveillance-society' model of security has become increasingly viewed as legitimate, with the result that there has been a considerable increase in the power of the state.[21] While formerly a degree of separation between those responsible for internal and external security was seen as essential to the preservation of democratic government, since September 11 it has become standard practice in the US and UK to assume that breaking down the legal and institutional barriers between law enforcement and security agencies is both practical and necessary, resulting in the emergence of an all-embracing concept of 'national security'.[22]

---

[19] Lyon, D, 'Surveillance Studies: Understanding Visibility, Mobility and the Phenetic Fix' (2003) 1(1) *Surveillance and Society* 3.

[20] This point has also been made by the group Privacy International. See 'Increased Abuse of Data and Disregard for Protections' (Privacy International press statement, 9 August 2004, available at http://www.privacyinternational.org (accessed 31 September 2006).

[21] Levi, M and Wall, DS, 'Technologies, Security, and Privacy in the Post-September 11 European Information Society' (2004) 31(2) *Journal of Law and Society* 203.

[22] This point is made clearly in a recent Department of Homeland Security press release: 'A critical obstacle to cooperation across the Federal government is to integrate data created by different agencies for different systems and different purposes.' See 'Secure Borders and Open Doors in the Information Age' (Department of Homeland Security fact sheet, 17 January 2006), available at http://www.dhs.gov/xnews/releases/press_release_0838.shtm (accessed 4 December 2006).

The removal of these barriers has serious implications for individual privacy. As many civil libertarians and privacy advocates have argued, as the surveillance power of the state expands, the number of truly private spaces available for individuals necessarily contracts, with the result that it becomes increasingly difficult for citizens to 'keep things to themselves'.[23] Furthermore, as Galison and Minow have observed, because legislation such as the Anti-terrorism Act and the USA PATRIOT Act helps to reinforce the view that it is worth sacrificing considerable amounts of privacy for the promise of security, it only exacerbates existing powerful anti-privacy trends in other areas of our social and economic lives:

> [F]ailures to attend to privacy in the design of technology, the articulation and enforcement of laws, and in the mechanisms of markets and politics produce downwards spirals, reducing both the scope of experiential privacy and people's expectation of and hope for privacy.[24]

The idea that individuals should be able to retain control over certain types of information about themselves and their dealings—and determine who has access to that information—underpins a number of different conceptions of the right to privacy.[25] It is also an idea that has to varying degrees found support in both British

---

In many respects, this new idea of 'national security' closely resembles the German concepts of *Staatssicherheit* or *Staatsschutz*. I am indebted to Eric Topfler for the observation that one additional consequence of this all-embracing approach to security is the tactical, as well as organisational, convergence of the police and the military. As security becomes a more important part of the national agenda, not only do we see a sharing of information and the development of stronger organisational links between the police and the security services, but also domestic security bodies 'borrowing' weapons and tactics from the military and others more traditionally associated with external, international defence.

[23] See, for example, Stanley, J and Steinhardt, B, 'Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society' (ACLU Technology and Liberty Program, 2003).

[24] Galison and Minow (2005), note 1 above, 258.

[25] For a defence of this particular view of privacy, see Fried, C, *An Anatomy of Values* (Cambridge, Harvard University Press, 1970); and Parent, W, 'Privacy, Autonomy, and Self-Concept' (1983) 24 *American Philosophical Quarterly* 81–89. A critique of this approach to privacy, or at least Parent's

and American law. Yet while it is clear that the pursuit of security poses a threat to this aspect of privacy, in the remaining sections of this chapter it will be argued that there are deeper issues at stake than the loss of what we may call 'informational privacy'. Privacy, it will be argued, is not simply about the keeping of secrets or the restriction of access to information. Rather, it is also about maintaining a degree of control over one's identity—an endeavour that is by nature much more indefinable and fluid but also goes to the heart of what it is to be human/maintaining human dignity.

CHANGING NOTIONS OF IDENTITY: NARRATIVES AND CATEGORIES

One of the central challenges of the modern state has been to find ways in which to identify citizens.[26] Passports, identity cards and social security numbers all represent attempts to ensure that each individual is readily and unmistakably distinguishable from others. Without stable identities and reliable mechanisms for identification, it is difficult for states to exercise any hold over those who live within their borders, or to ensure that they are able to protect against internal and external threats.[27] At a more mundane level, reliable methods of identification are also essential to the running of anything other than the most minimal state. As Rose has observed, although

---

account of it, can be found in DeCew, J, *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology* (Ithaca, Cornell University Press, 1997).

[26] This problem has not been confined to the state but also confronts private organisations. In order to highlight the relationship between state security and surveillance, however, in this chapter the primary focus will be on states and their attempts to document the identity of individuals.

[27] See Higgs, E, 'The Rise of the Information State: The Development of Central State Surveillance of the Citizen in England, 1500–2000' (2001) 14(2) *Journal of Historical Sociology* 175–97; and Torpey, JC, *The Invention of the Passport: Surveillance, Citizenship and the State* (Cambridge, Cambridge University Press, 2000).

individuals may at times resist, participation in modern society necessarily involves allowing oneself to be identified and, more crucially, classified:

> It is impossible to participate in almost any contemporary practice without being prepared to demonstrate identity in ways that inescapably link individuation and control. The modes of identification are multiple: computer-readable passports, driving licenses with unique identification codes, social insurance numbers, bank cards, credit cards… Each card identifies the bearer with a virtual identity—a database record storing personal details—whilst at the same time allowing access to various privileges.[28]

As anyone who has tried to open a bank account or obtain a licence to drive a car knows, it is almost impossible to live a normal life without some form of officially recognised identification document. Furthermore, we have come to accept that government agencies and private companies regularly obtain, keep and exchange information about us, often with a view to classifying us according to given sets of characteristics. For example, most people now regard it as normal and reasonable for the state to inquire about such things as an individual's employment status, level of income and marital status, particularly if that individual is seeking welfare subsidies, tax relief or some other kind of state benefit.[29] Equally, we willingly disclose information about our assets, financial liabilities and spending habits to banks in order to receive loans, mortgages and credit cards. Having to share personal information is widely understood to be one of the prices we pay in order to participate in society and enjoy many of the benefits the modern state has to offer.

While most people may not feel particularly concerned about having to tell the government exactly how many children or other dependents they might have, or inform a bank the amount of money they spent on loan repayments in the previous

---

[28] Rose, N, *Powers of Freedom: Reframing Political Thought* (Cambridge, Cambridge University Press, 1999) 240–41.

[29] Gilliom, J, 'Struggling with Surveillance: Resistance, Consciousness and Identity' in K Haggerty and R Ericson (eds), *The New Politics of Surveillance and Visibility* (Toronto, University of Toronto Press, 2006) 111–40.

year, many are unaware of just how much the state and private sector companies actually know about them. In part, this is due to the fact that as we make more and more use of technologies like the mobile phone, credit cards and the internet, we leave behind us digital trails that may contain a wealth of personal information. If you shop online with any degree of regularity, you reveal not only your address but over time also various consumption preferences and possibly information about your credit worthiness. In addition, thanks to the spread of new and increasingly sophisticated surveillance techniques and technologies—such as CCTV cameras, internet cookies and computer spyware—many of our activities are now monitored without our knowledge and information collected without our consent.

This intensification in the level of state and private surveillance has had two distinct effects. First, in countries such as the US and the UK, it has led to a significant reduction in levels of personal privacy and confidentiality. This is something that numerous commentators have drawn attention to in recent years, with the result that many contemporary critiques of surveillance focus almost exclusively on the negative implications of new surveillance technologies.[30] Secondly, the intensification of surveillance has also transformed the way in which individuals are viewed and treated by the state and an increasing number of private organisations.

As surveillance has become more widespread (and information and communication technologies more efficient), the process of individual classification has become vastly more sophisticated. For example, whereas in the past government agencies may have been limited to using relatively simple categories when attempting to identify and distinguish between citizens, with the advent of computerised

---

[30] For an example of such an account, see Davies, S, *Big Brother: Britain's Web of Surveillance and the New Technological Order* (London, Pan Books, 1996).

databases and automated data-matching techniques, they are now capable of cross-referencing large amounts of personal information and drawing extremely fine-grained individual distinctions. No longer are individuals sorted according to a handful of basic criteria such as gender, date and place of birth, income level and marital status. Instead, governments and private organisations are able to build profiles based on hundreds of separate pieces of information—such as how many cars someone owns or what periodicals he or she subscribes to—and instantly modify those profiles as new information becomes available. Equally, companies like Amazon.com that use software that relies on records of past purchases to make product recommendations to their regular customers can over time develop customer profiles that are extremely textured and eerily accurate in their ability to predict future preferences, a fact hailed with pride by the company's founder, Jeff Bezos:

> We not only help readers find books, we also help books find readers, with personalized recommendations based on the patterns we see. I remember one of the first times this struck me. The main book on the page was on Zen. There were other suggestions for Zen books, and in the middle of those was a book on how to have a clutter-free desk. That's not something that a human editor would have ever picked. But statistically, the people who were interested in the Zen books also wanted clutter-free desks. The computer is blind to the fact that these things are dissimilar in some way that's important to humans. It looks right through that and says yes, try this. And it works.[31]

The growing use and sophistication of surveillance-based methods of individual classification has important implications for the relationship between the individual and the state. More specifically, a tension has emerged between two fundamentally opposed conceptions of identity: the narrative and the categorical. According to Ricoeur, individuals typically seek to make sense of their own identities by constructing narratives about themselves and those around them, and it is through

---

[31] Quote taken from a *Wired Magazine* interview with Jeff Bezos. See Anderson, C, 'The Zen of Jeff Bezos', *Wired Magazine*, January 2005, available at http://www.wired.com/wired/archive/13.01/bezos.html (accessed 31 September 2006).

these narratives that an individual is able to develop a sense of self that is fluid and that recognises the existence and autonomy of others.[32] Drawing on Ricoeur, Dauenhauer has observed:

> We make sense of our own personal identities in much the same way as we do of the identity of characters in stories. First, in the case of stories, we come to understand the characters by way of the plot that ties together what happens to them, the aims and projects they adopt, and what they actually do. Similarly I make sense of my own identity by telling a story about my own life. In neither case is the identity like that of a fixed structure or substance. These identities are mobile… Until the story is finished, the identity of each character or person remains open to revision.[33]

In contrast to such narrative identities, categorical identities stress the importance of particular personal characteristics with a view to determining whether an individual belongs to some pre-defined group. Personal information is viewed as static and capable of being distilled into data, which can in turn be combined and used as the basis for making statements about an individual's character and—even more crucially for states concerned about issues of security—predictions about his or her future behaviour. Whereas the notion of narrative identity focuses on the uniqueness of individuals and their innate capacity to evolve and develop relationships with other people, the notion of categorical identity is based on the belief that human beings are capable of being summarised and understood in terms of lists. As Franko Aas has written,

> [A categorical] identity is not marked by its unique biography and a certain internal development, but is rather adjusted to the 'computer's ontology': composed of items of information that like Lego bricks can be taken apart and clearly understood as well as fit with other items of information in new configurations.[34]

---

[32] See, inter alia, Ricoeur, P, 'Reflections on a New Ethos for Europe' (1995) 21(5) *Philosophy and Social Criticism* 6.

[33] Dauenhauer, B, 'Paul Ricoeur' in EN Zalta (ed), *The Stanford Encyclopedia of Philosophy*, Winter 2005 edn, available at http://plato.stanford.edu/archives/win2005/entries/ricoeur (accessed 11 December 2006).

[34] Franko Aas, K, 'From Narrative to Database: Technological Change and Penal Culture' (2004) 6(4) *Punishment and Society* 386.

In part, the tension between these two notions of identity can be traced to the emergence of the modern bureaucratic state. Indeed, the categorical identity has its origins in the nineteenth-century paper file, which was a crucial tool in the first systematic attempts by governments to identify and collect information about individuals. During the first half of the twentieth century, for those concerned about the growth of state power and the dangers of totalitarianism, the file came to be seen as deeply symbolic of the dehumanising nature of bureaucracy and the struggle for individual freedom. Although it is now common to regard Orwell's novel *1984*, in which privacy is non-existent, as merely a dystopic vision, it can also be interpreted as an account of what happens when it is the state, rather than individuals, who makes even basic decisions about identity.

Regardless of how someone chooses to define himself or herself, or how individuals are seen by those who know them personally, in the modern state it is the file that forms the basis of all administrative decision making. Furthermore, because it is necessary for the state to assume that the information contained in an individual's file is accurate, the categorical or administrative identity that emerges from that file must be preferred to any alternative narrative account. Someone may regard herself, for example, as a good mother who has made a new life for her children by moving to another country and earning money by cleaning other people's houses. For the state, however, if the information contained in a file says otherwise, then it is the categorical identity that will ultimately prevail: this same person is a single parent, unemployed and an illegal immigrant.

Although most people probably do not think of their relationship to the state (or private organisations) in terms of a competition between their own narrative accounts of themselves and some categorical identity that is constructed for them, this

is largely because until very recently categorical identities and their real effects on everyday life have been relatively limited. These two conceptions of identity only come into competition when the categorical overlaps, contradicts and supplants the narrative, and so long as categorical identities are based on a narrow range of information, the possibility of such conflict remains limited. Yet as governments collect more and more personal information and as advances in information and communications technology make it easier to store, process and retrieve that information, the complexity and scope of the categorical identities they construct gradually increases, as does the potential for conflict with other conceptions of identity.

While personal narratives for most part remain the dominant means by which we understand identity in modern society, four related developments—all of which are taking place against a growing obsession with issues of security—have led to increased competition and conflict between narrative and categorical identities. First, advances in surveillance technology and techniques now make it possible for governments to collect many previously unavailable forms of information, such as digital recordings of activities in public (via CCTV), information about activities online (via surveillance programmes such as Carnivore) and records of communications between people (via mobile phone records, email, etc).

Second, developments in information technology have made it much easier for government agencies to share such information amongst themselves and with private institutions, and to draw additional information from the public domain. With the advent of sophisticated search engines, it is now possible for government officials and company employees to access large amounts of information about an individual from a vast array of sources. Furthermore, the ability to replicate and share digital

information has meant that the idea of the single, comprehensive file has become largely redundant. Instead, categorical identities are increasingly based on the convergence of many separate bodies of information, all of which are brought together by a single identifier—such as a national insurance or social security number.

Third, advances in data matching and the development of so-called 'algorithmic surveillance' techniques have made it possible to automate many decision-making processes that rely on categorical identities.[35] Systems such as the American Computer Assisted Passenger Pre-screening System (CAPPS) programme are a good example of this, as are online application forms that compare the information submitted by an individual against multiple databases before making a decision on whether that individual is entitled to a particular welfare benefit or is required to pay more tax.

Finally, the failure of existing privacy and data protection frameworks to keep pace with these developments has meant that many individuals are unable to determine what exactly the state knows—or thinks it knows—about them. It is therefore difficult for individuals to contest with effectiveness the categorical identities that have been constructed for them.

Although not all of these developments are technologically determined, they can clearly be traced to recent advances in surveillance, information processing and digital communication. In the past such advances were largely driven by the desire of governments to streamline decision-making and improve administrative efficiency. However, the extremely detailed, textured profiles of citizens that are now available to

---

[35] See Norris, C, 'Algorithmic Ssurveillance' (1995) 20 *Criminal Justice Matters* 7–8; and Norris, C, Moran, J and Armstrong, G, 'Algorithmic Surveillance: The Future of Automated Visual Surveillance' in C Norris, J Moran and G Armstrong (eds), *Surveillance, Closed Circuit Television and Social Control* (Ashgate, Aldershot, 1998) 255–76.

states hardly seem necessary merely to distinguish individuals from one another for the purposes of tax, benefits, voting, etc. Instead, since 9/11, it is security—defined in terms of the ability of the state to protect its citizens from internal and external threats—that is the primary rationale for increasing levels of state surveillance and improving data-sharing. This has resulted in the rapid, simultaneous expansion and convergence of surveillance networks and databases in countries such as the US and UK.

Categorical identities have moreover become increasingly important, as they provide the basis for assessments of risk and pre-emptive measures aimed at increasing security. Perhaps the best example of this is the growing use of algorithmic surveillance in airports. Each time a passenger passes through airport security, various databases are drawn together, his or her categorical identity is reconstructed and automatically scrutinised, and then that identity is used to determine whether the passenger represents a threat to security. Passengers who are classified as such a threat can suddenly find themselves subjected to additional searches, questions and possible detention. Rarely, if ever, are individuals told why they are considered to be 'high risk', nor are they given opportunities to query the information or decision-making process that led to their 'high risk' classification. Once such a categorical identity has been established, it trumps all other competing accounts of the individual, at least insofar as matters of security are concerned.[36]

---

[36] It is important to note that the distinction between narrative and categorical identities can never be an absolute one. Clearly, some markers of identity that are typically used as the basis for the construction of categorical identities, such as race, can be self-defined and, as such, are products of personal narratives. As a consequence, although acknowledging the basic distinction between narrative and categorical identities is necessary if we are to fully understand the threat posed by various forms of surveillance and security measures, the line between the two is inevitably indistinct (particularly where a personal narrative is informed by official classification processes).

The growing reliance on categorical identities has many serious implications.[37] As Calhoun has observed, the use of categorical identities has a tendency to produce repressive and discriminatory outcomes because the very notion of categorical identities favours sameness over difference and regards identity as a function of membership of a group:

> [The imposition of categorical identities] allows a kind of abstraction from the concrete interactions and social relationships within which identities are constantly renegotiated, in which individuals present one identity as more salient than another, and within which individuals achieve some personal sense of continuity and balance among their various sorts of identities… The abstractness of categories encourages framing claims about them as though they offer a kind of trump card over the other identities of individuals addressed by them. This encourages an element of repression within the powerful categorical identities.[38]

As a case in point, a bank manager who must decide whether or not to grant a personal loan may not be willing (or allowed) to take into consideration the applicant's own account of his or her financial history; but the bank manager will almost certainly base the decision on a categorical identity made up of the applicant's credit rating, account history, employment status, etc. Even if the manager believes the applicant is sincere when he or she promises to repay the loan on time, and even if the manager believes the applicant has the means to do so, the categorical identity will almost certainly remain the primary determinant, and the loan may be refused.

---

[37] One reason why categorical identities may have become more prominent in recent years—at least in terms of their use by the state and law enforcement agencies—is due to the declining use of 'human intelligence' since the end of the Cold War. Technological advances that have made electronic surveillance easier and cheaper have combined with a general 'technological ideology' to shift resources away from the use of human agents—such as informants and eavesdroppers—towards greater and greater financial and organisational investment in sophisticated surveillance devices and computer software. As a result, in many instances categorical identities become increasingly important simply because there are no available alternatives. I am indebted to Kevin Haggerty for this observation.

[38] Calhoun, CJ, *Critical Social Theory: Culture, History, and the Challenge of Difference* (Oxford, Blackwells, 1995) 220–21.

Aside from having the effect of reducing the applicant to a handful of numerical indicators, this process of decision-making is extremely hard to challenge.[39] Regardless of how implausible the categorisation, it typically is not the organisation that utilises the classification who must justify decisions but rather the individual in question who must prove that he or she been wrongly identified—as someone who is a credit risk, who requires regular tax audits, who should be on a no-fly list, etc. Furthermore, as the number of databases increases and the linkages between them become more complex and well established, it also becomes difficult for individuals to determine why they have been classified in a particular way in the first place. Credit records are, for example, now based on information drawn from a vast array of sources, making it extremely difficult for the average person to uncover where any 'black mark' may have come from.[40]

Taken to an extreme, the use of sophisticated categorical identities by the state and private companies has the potential to undermine the way in which ordinary individuals understand themselves. Confronted with a world in which identity is increasingly defined according to the information contained in databases, where

---

[39] Of course, it is important not to take the argument in favour of the narrative identity too far. The point here is not to suggest that we should rely only on narrative identities and ignore other information but rather to caution against the unquestioning reliance on categorical identities and the temptation of using them as trumps in decision-making. I am grateful to Simon Cole for alerting me to the danger of privileging personal narratives and thereby lapsing into 'wishy-washy humanism'.

[40] Furthermore, as David Philips has usefully observed, although in many jurisdictions insurance companies and banks are obliged to reveal the information that they have used to reach decisions about offering insurance or providing loans, they are not required to disclose the algorithms that attribute relative weight and then categorises individuals according to that information. See Phillips, D, 'Privacy, Surveillance, or Visibility: New Information Environments in the Light of Queer Theory', Paper presented at the annual meeting of the International Communication Association, New York City, available at http://www.allacademic.com/meta/p12412_index.html (accessed 11 December 2006).

routine decisions are made by algorithms rather than by people, it becomes progressively more difficult for individuals effectively to assert alternative visions of themselves.[41] If an 'intelligent' data-matching process that draws on a vast array of interconnected databases determines that I am a potential security risk, how do I deny this? Do I question the information on which the decision is based? The decision-making process itself? What if the information is correct and the decision is, on its face, reasonable, but wrong?[42] How do I explain, for example, that although I may have been interested in extremist politics as a student, I have now disavowed them? Or even more problematically, how do I argue that I still subscribe to radical political ideas but am not a terrorist risk because of a commitment to non-violence? Like a criminal record, the categorical identity has the potential to rob individuals of the right to define themselves beyond its confines and to develop as individuals.[43]

Although various social, political and technological changes have contributed to the growing importance of categorical identities over the past forty years,

---

[41] This is a point that has also been made by Philip N Howard, who has suggested that, by its very nature, 'electronic technology may favour categorical identities more than dense social networks.' See Howard (2003) 219.

[42] One response to this question—and to many of the concerns raised about the use of categorical identities in this chapter—is to suggest that the problem lies not with the use of categories per se but rather with the fact that they are simply not detailed enough. If, for example, the state knew a great deal more about us than it does now and was therefore able to construct even more sophisticated categorical identities for each of us, would or should we object? I am grateful to Kevin Haggerty for raising this line of questioning. Although it is beyond the scope of this chapter to consider the argument in full, one response might be that the cost in terms of privacy that we would have to surrender in order for such a category to be constructed would simply outweigh the benefits of having more accurate, and only possibly less reductive, categorical identities.

[43] Taking this argument to its extreme, categorical identities can generate digital shadows of ourselves—or as Deleuze prefers to call them, 'dividuals'—that are stored within databases and can be created, altered and shared without our knowledge or consent. See Deleuze, G, 'Postscript on the Societies of Control' (1992) 59 *October* 3.

developments since September 11 threaten to tip the balance even more in favour of categorical identities. Looked at through a different lens, it is also possible to characterise these changes in terms of the demise of administrative discretion and the emergence of a deep organisational reliance on automated decision-making. Legislation such as the PATRIOT Act and the Anti-Terrorism Act is significant not only because it seeks to remove barriers to information sharing and to promote co-operation between law enforcement agencies, but also because it helps to reinforce the view that categorical identities based on information obtained through surveillance and generated by data-matching techniques, are the only appropriate basis of state–individual interaction. The pursuit of security along these lines is dangerous not simply because it undermines claims to individual privacy, but because it threatens to normalise and make ubiquitous a way of constructing identity that is inherently dehumanising and has the potential to institutionalise various forms of cultural and ethnic discrimination.

Faced with a growing emphasis on security and a steadily expanding network of state and commercial surveillance, what chance do we have for resisting the shift from narrative to categorical constructions of identity? The most obvious answer to this question is of course to bolster existing privacy protections with a view to making it more difficult for the state and private companies to acquire and share personal information. However, many of the agencies and institutions that represent a threat to privacy are powerful, well-funded and closely integrated into larger state systems. Any attempt to limit them is therefore unlikely to be very effective. This is a point that is well-illustrated by the recent case of the Total Information Awareness (TIA) programme in the United States, which aimed at vastly improving the US government's data mining capacities. Although the Defence Advanced Research

Projects Agency (DARPA) was forced by Congress to suspend development of the TIA system following an outcry from civil libertarians and journalists, there can be little doubt that many of the activities planned for the TIA are now being performed by other government agencies.[44] As Galison and Minow have observed,

> Like a ball of mercury, the data-mining activities scatter and grow less visible once subjected to pressure. Public concerns about privacy have generated more secrecy about the government activities that jeopardise personal privacy.[45]

Given the difficulty of comprehensively protecting privacy interests through legislation and regulation, it is clear that a multi-pronged strategy is necessary to respond effectively to the growing obsession with security and surveillance. Legal and institutional reform must be accompanied by other measures that are designed to foster a general respect for privacy and to mitigate the de-humanising effects of categorical identities. With this larger aim in mind, the following section will consider several models of privacy and their implications for both security and personal identity.

PRIVACY, IDENTITY AND INFORMATIONAL SELF-DETERMINATION

The Value of Privacy

Privacy rights are notoriously difficult to define, in part because they often overlap with other substantive rights—such as the right to liberty—that are both well-established and well-defined, and also because there is often dispute over what it is

---

[44] One of the major opponents of the TIA was the American Civil Liberties Union (ACLU), which argued that the sort of data-mining programme envisaged for the TIA would 'amount to a picture of your life so complete it's equivalent to somebody following you around all day with a video camera.' See Baer, S, 'Broader US Spy Initiative Debated; Poindexter leads Project to Assess Electronic Data, Detect Possible Terrorists; Civil Liberties Concerns Raised', *Baltimore Sun*, 5 January 2003, 1A (quoting Jay Stenley of the ACLU).

[45] Galison and Minow (2005) 266.

that privacy seeks to protect.[46] According to Thomson, a leading proponent of the right to privacy, it is impossible to define privacy because the right to privacy is in fact composed of a cluster of other rights, typically property rights and the right to bodily integrity.[47] As such, when we claim that our privacy has been violated, what we really mean to say is that some other substantive right has been infringed upon. In this sense, privacy is a fundamentally derivative concept.[48]

One approach to the question of defining privacy is to regard privacy as the control of personal information.[49] In Westin's now famous book *Privacy and Freedom*, he argues that privacy is fundamentally concerned with the ability of 'individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others'.[50] This view has recently been taken further by Parent, who suggests that one of the fundamental conditions of privacy is the ability to prevent others from acquiring or holding undocumented personal information about oneself.[51] For Parent, such personal

---

[46] Feldman, D, 'Secrecy, Dignity or Autonomy? Views of Privacy as a Civil Liberty' (1994) 47(2) *Current Legal Problems* 41; Feldman, D, 'Privacy-related Rights and their Social Value' in P Birks (ed), *Privacy and Loyalty* (Oxford, Clarendon Press, 1997) 15. See also arguments by Ronald Dworkin concerning the problems inherent in the relationship between privacy and liberty: Dworkin, R, *Taking Rights Seriously* (London, Duckworth, 1977) 266–78.

[47] Thomson, J, 'The Right to Privacy' (1975) 4 *Philosophy and Public Affairs* 295–314.

[48] *Ibid*. For a detailed critique of this position, see Scanlon, T, 'Thomson on Privacy' (1975) 4 *Philosophy and Public Affairs* 315–22; and Inness, J, *Privacy, Intimacy and Isolation* (Oxford, Oxford University Press, 1992).

[49] See for example: Westin, A, *Privacy and Freedom* (New York, Atheneum, 1967); Fried (1970); and Parent, W, 'Privacy, Morality and the Law' (1983) 12(4) *Philosophy and Public Affairs* 269–88. For a brief synopsis of Westin's work on privacy, see DeCew, J, 'Privacy' in EN Zalta (ed), *The Stanford Encyclopedia of Philosophy*, Fall 2006 edn, available at http://plato.stanford.edu/archives/fall2006/entries/privacy (accessed 11 December 2006).

[50] Westin (1967) 7.

[51] Parent (1983).

information is necessarily factual and includes such things as details about one's health, marital and financial status, educational background and sexual orientation. While he does not go so far as to claim that there is a clear legal or moral right to privacy, Parent makes clear that the loss of control over such personal information can lead to far-reaching consequences and very real effects for the lives of individuals:

> [I]f others manage to obtain sensitive personal knowledge about us they will by that very fact acquire power over us. Their power could then be used to our disadvantage. The possibilities for exploitation become very real. The definite connection between harm and the invasion of privacy explains why we place a value on not having undocumented personal information about ourselves widely known.[52]

In contrast to this emphasis on the control of information, other writers have suggested that privacy is best understood in terms of its connection to ideas of personal autonomy, self-determination and human dignity. This approach, which frequently leads to privacy being framed in terms of the right to a private or family life, has tended to dominate legal discussion of privacy in both the US Supreme Court and the European Court of Human Rights. Privacy in this sense goes well beyond control over information and looks to provide individuals with the means to protect themselves against intrusions that might compromise their independence and represent an affront to their sense of human dignity.

According to Feldman, privacy rights are important because they enable individuals and groups to determine and, to some extent at least, control the boundaries between different interlocking social spheres.[53] In this regard, he argues, it is important to recognise the communitarian aspects of the idea of privacy. If we view society as a 'community of communities', made up of groups with different memberships that may or may not overlap, then privacy provides the mechanism by which these groups are able to preserve their independence while also interacting with

[52] *Ibid*, 276.

[53] See Feldman (1994) 41; and Feldman (1997) 15.

one another. At the individual level as well, a notion of privacy is valuable insofar as it enables us to limit the extent to which we are subjected to the demands and judgments of others.

Within this framework, privacy rights deserve protection because they are essential for the maintenance of personal autonomy and enable individuals to maintain a range of different and valuable social relationships.[54] If we are constantly required to respond to the expectations of those around us, our choices are unlikely to be free, nor are we likely to develop a capacity for self-determination or a degree of self-fulfilment. Privacy is hence essential for the establishment and maintenance of a unique sense of self. Indeed, as Galison and Minow have observed, privacy and the construction of personal identity are intimately connected:

> Even though its meanings are multiple and complex, privacy in closely connected with the emergence of a modern sense of self. Its jeopardy signals serious risk to the very conditions people need to enjoy the kind of self that can experiment, relax, form and enjoy intimate connections, and practice the development of ideas and beliefs for valued expression.[55]

Of course, these two approaches—privacy as the control of information and privacy as the protection of individual autonomy—are not entirely incompatible with one another. If one views control over personal information not merely in terms of a narrow conception of ownership or of secrecy but rather as essential to the maintenance of individual autonomy and dignity, then it follows that spheres of privacy are as much about controlling how information about oneself is communicated to the outside world as it is about controlling who has access to us and our activities. After all, as Lustgarten and Leigh argue, the collection of personal information without an individual's consent can amount to a serious affront to human dignity and demonstrate an absence of respect for their need for personal autonomy:

---

[54] Feldman (1994) 53–59.

[55] Galison and Minow (2005) 258.

> Imagine being unable to draw the curtain in your bedroom, so that others can see you naked at any time of their choosing. The fear and revulsion this image evokes has little to do with the beauty or otherwise of one's body, but everything to do with one's sense of *self*. If I have no control over what is known about me, I am seriously diminished as a person both in my own eyes and in those which are capable of intruding upon me.[56]

If we accept this view of privacy, then it follows that there is a clear relationship between privacy and the construction of personal identity. As we move from very private spheres (for example, the home) into increasingly less private ones (such as the workplace), each step requires us to surrender some amount of control over information about ourselves, information that can then be shared and its meaning potentially transformed. The more public my activities, the more susceptible they are to being known, interpreted and judged by others, with the result that my capacity to define myself—to construct my own narrative identity or to resist a categorical identity that might be imposed upon me by the state—diminishes. This is of course one of the reasons why we often feel most secure in the context of the home. It is not simply because we have considerable control over the space around us, but also because we can more or less be who we want to be.

Privacy rights are valuable then not simply because they are essential to the maintenance of personal autonomy or the defence of human dignity, or even because they endow us with some modicum of control over information about ourselves. Privacy is important because of its relationship to the construction of identity and because of the way in which it helps us to develop and defend particular visions of self. In making a demand for privacy, we reassert control over information about ourselves and make it more difficult for those who would seek to categorise us or reduce our identity to a list of particular traits or characteristics.

---

[56] Lustgarten, L and Leigh, I, *In from the Cold: National Security and Parliamentary Democracy* (Oxford, Clarendon Press, 1994) 39–40.

An Expanded Model of Privacy

The relatively broad conception of privacy outlined above may go some way in drawing a connection between privacy and human dignity—and hence human rights—but it is unlikely on its own to provide an adequate basis for resisting the pressures of security and the attendant drive from narrative to categorical notions of identity. There are two reasons for this. First, central to even the broadest conception of privacy is the assumption that it is possible to agree on what constitutes personal information deserving of protection. Yet as Nissenbaum has argued, the meaning of any piece of information is at least in part determined by its context and the manner in which it is disclosed. The fact that I choose to behave or present myself in a certain way in one context does not mean that I intend to be defined by behaviour and identity in all other contexts. As Schoeman has rightly observed,

> A person can be active in the gay pride movement in San Francisco, but be private about her sexual preferences vis-à-vis her family and co-workers in Sacramento. A professor may be highly visible to other gays at the gay bar but discreet about sexual orientation at the university. Surely the streets and newspapers of San Francisco are public places as are the gay bars in the quiet university town. Does appearing in some public settings as a gay activist mean that the person concerned has waived her rights to civil inattention, to feeling violated if confronted in another setting?[57]

In a world in which surveillance is becoming ubiquitous and information can be transmitted almost instantaneously to a multitude of people at virtually zero cost, it is exceptionally easy for that information to be divorced from its context and for it to take on new and unexpected meanings. As a consequence, if we are to maintain any sense of privacy or control over how our identity is constructed, it is important to develop a concept of privacy that recognises that the meaning of information is

---

[57] Schoeman, F, 'Gossip and Privacy' in RF Goodman and A Ben-Ze'ev (eds), *Good Gossip* (Lawrence, University Press of Kansas, 1994) 73 (quoted in Nissenbaum, H, 'Privacy as Contextual Integrity' (2004) 79(1) *Washington Law Review* 101–39, 122).

heavily context dependent and can easily be transformed, abused and/or misinterpreted.

Nissenbaum has suggested that the solution to this problem is to develop a model of privacy that is capable of maintaining 'contextual integrity', which is defined as 'compatibility with presiding norms of information appropriateness and distribution'.[58] According to this principle, we should move away from thinking about privacy in terms of dichotomies—such as sensitive and non-sensitive information, or distinctly private and distinctly public spaces—and instead recognise that all areas of life are subject to flows of information:

> Observing the texture of people's lives, we find them not only crossing dichotomies, but moving about, into, and out of a plurality of distinct realms. They are at home with families, they go to work, they seek medical care, visit friends, consult with psychiatrists, talk with lawyers, go to the bank, attend religious services, vote, shop, and more. Each of these spheres, realms, or contexts involves, indeed may even be defined by, a distinct set of norms, which governs its various aspects such as roles, expectations, actions, and practices. For certain contexts, such as the highly ritualized settings of many church services, these norms are explicit and quite specific. For others, the norms may be implicit, variable, and incomplete (or partial)… Contexts, or spheres, offer a platform for a normative account of privacy in terms of contextual integrity.[59]

The second, related reason why many existing models of privacy are unable to respond to the challenges of modern surveillance and the current overwhelming drive for security is that they—unlike many of the technologies that now threaten privacy—are rooted in an increasingly anachronistic view of the distinction between the public and the private. Modern information flows do not respect traditional physical boundaries: for example, when I surf publicly accessible internet sites in the privacy of my own home, am I moving in a private or a public domain? Moreover, many state institutions now draw on personal information that is collected by the private sector or has otherwise found its way into the public domain. As a consequence, privacy

---

[58] Nissenbaum (2004) 137.

[59] *Ibid*, 119–20.

protections that can only be enforced against public bodies—such as the data protection provisions currently in operation in the United Kingdom—are severely limited in their application.[60]

In light of these difficulties, it is clear that if we are concerned about privacy and the effect that the current obsession with security is having on our ability to maintain control over our own identities, we must develop a new vision of privacy that recognises the importance of context and the increasing irrelevance of traditional notions of the public/private divide. The language and discourse of privacy must, as a basic starting point, acknowledge the deep connection between information and identity, while privacy protections must recognise that the meaning of information and informational norms—that is, the norms of appropriateness and distribution—vary according to context. Such a vision of privacy would represent a significant departure from the models that underpin the privacy and data protection laws of the US and UK. Furthermore, it almost certainly represents a departure form the way in which most people think about questions of privacy in their everyday lives. Yet just as we have come to accept that the nature and extent of surveillance has changed in recent years, so too must society begin to think more creatively and radically about the concept of privacy and the value of identity.

Informational Self-determination

Assuming that we are prepared to embrace a concept of privacy such as that outlined above, the question then arises as to how best to protect the privacy interests that arise from such a model. It is tempting to assume that all that is needed to achieve

[60] Furthermore, given the pressures associated with the pursuit of security, it makes little sense to entrust the state—via the courts or some external agency such as the Office of the Data Protection Commissioner—to both define and then police the boundary between the public and the private.

this are more expansive privacy laws. However, as Galison and Minow have argued, it may be possible to enact legislation that discourages the state from invading the privacy of individuals, but it is impossible to construct a system of laws that will provide for the complete protection of privacy or resolve the inevitable conflict between privacy and the demands of security.[61] Instead, what is needed is a multi-dimensional strategy that not only seeks to transform the way in which the law defines and protects privacy, but also generates a general demand for privacy within society:

> Without deliberate effort [to promote privacy] a downward spiral can become a vicious circle, eroding privacy through legal permission, technological access to unprecedented amounts of personal information, and diminishing public expectations of privacy. Deliberate initiatives in law, technology, and market and educational strategies designed to generate desire could, in contrast, promote an upward spiral, moving up while rotating back and forth between positive desires on the one side and legal/technological constraints on the other.[62]

Although it is well beyond the scope of this chapter to outline a comprehensive strategy for the promotion of individual privacy, one way in which privacy could be enhanced in the US and the UK is the introduction of a free-standing right to informational self-determination. Insofar as such a right would increase the amount of control that individuals are able to exercise over personal information, its introduction would constitute an important step towards the development of a vision of privacy that properly recognises the fluid and contextual nature of information in modern society.

As has already been noted, in order to resist the unwanted imposition of a categorical identity, it is crucial that individuals are able to determine or at least have a say in what sorts of personal information are held by the state and, even more importantly, how that information is used. While data protection laws go some way to providing this, they typically focus on only regulating the manner in which

---

[61] Galison and Minow (2005) 260.

[62] *Ibid*, 261.

information is acquired; the protection they offer to individuals is therefore limited. Once information has been shared and is in the public domain, individuals may be able to take action against the body that 'leaked' the information, but there is little they can do to prevent others from dealing in their personal information or passing it on. Consequently, what is needed in addition to data protection is some recognition that individuals 'own' information about themselves and should consequently have control about over what is ultimately done with that information.

For an example of how a right to informational self-determination might work in practice, one need only go so far as Germany, which legally recognised such a right over twenty years ago. In 1983, it was held by the Federal Constitutional Court that all German citizens have a right to what was referred to as 'informational self-determination'. Derived from Articles 1(1) and 2(1) of the Basic Law,[63] the right is regarded as a personal right (*Persönlichkeitsrecht*) and is limited only by the 'predominant public interest.' In justifying the establishment of this new right, the court was clear in its desire to link issues of autonomy with control of information and the development of self:

> Who can not certainly overlook which information related to him or her is known to certain segments of his social environment, and who is not able to assess to a certain degree the knowledge of his potential communication partners, can be essentially hindered in his capability to plan and to decide. The right of informational self-determination stands against a societal order and its underlying legal order in which citizens could not know any longer who what and when in what situations knows about them.[64]

---

[63] According to Art 1(1) of the Basic Law for the Federal Republic of Germany (Grundgesetz), 'Human dignity shall be inviolable. To respect and protect it shall be the duty of all state authority.' Further to this, Article 2(2) states: 'Every person shall have the right to free development of his personality insofar as he does not violate the rights of others or offend against the constitutional order or the moral law.'

[64] BVerfGE 65, 1.

Clearly, this German conception of the right to informational self-determination goes a long way in addressing many of the concerns raised by Nissenbaum about the need to acknowledge the contextual dimension of personal information.[65] In addition, it avoids one of the great ironies of traditional privacy rights—that individuals are required to identify what they regard as private in order to protect themselves from unwanted intrusions, despite the fact that the mere act of claiming something is private tells the state that it is something the individual regards as valuable. The German formulation, however, reverses this burden by requiring the state—or any other user of personal information—to justify why the use does not infringe upon an individual's autonomy and his or her expectation to be able to control how that personal information is used. Finally, the right to informational self-determination has the advantage of not being contingent on transgressions of some imagined boundary between private and public space; it is therefore better equipped to protect individual interests in a world of information flows.

---

[65] It is important to note, however, that concerns about the scope of the right to informational self-determination and the operation of the public interest exception have been raised by a number of German commentators. According to Wolf-Dieter Narr, for example, in recognising the right to informational self-determination the Federal Court has in effect helped to pave the way for what he refers to as 'Vorwärtsverrechtlichung' or 'forward-legislation'. For Narr, regulation designed to ensure that police and security services are acting in the public interest have ironically led to a situation in which there has been an increase in police powers and what has been described by various commentators as an 'over-regulated absence of regulation'. On these points, see: Narr, W-D, 'Wir Bürger als Sicherheitsrisiko: Rückblick und Ausblick' (1998) 60 *Bürgerrechte & Polizei/CILIP* 30–40, available at http://www.cilip.de/ausgabe/60/narr60.htm (accessed 31 September 2006); Pütter, N et al, 'Bekämpfungs-Recht und Rechtsstaat. Vorwärtsverrechtlichung in gebremsten Bahnen?' (2005) 82 *Bürgerrechte & Polizei/CILIP* 6–15; Kutscha, M, 'Auf dem Weg zu einem Polizeistaat neuen Typs? (2001) *Blätter für deutsche und internationale Politik* 214–21, available at http://www.blaetter-online.de/archiv.php?jahr=2001&ausgabe=02 (accessed 4 December 2006); and Roggan, F, *Auf dem legalen Weg in einen Polizeistaat. Entwicklung des Rechts der Inneren Sicherheit* (Bonn, Pahl-Rugenstein, 2000).

Given the existence of this right, it is perhaps unsurprising that despite similar calls for an expansion in state surveillance and the extension of existing security legislation, no equivalent of the PATRIOT Act or the Anti-terrorism Act has as yet been enacted in Germany. In the face of a strong constitutional commitment to the idea that individuals have a right to determine how information about themselves is used, it is difficult for the government, regardless of the public mood, to centralise the collection of personal details and remove institutional checks on the sharing of information in the way that has occurred in the US and UK since 9/11. Recognising such a right in the US or UK context may not provide an unassailable defence against the excessive surveillance demands of the state or the growing use of categorical identities, but it deserves serious consideration if only because it would add a new and substantial level of protection for privacy at a time when other protections are either failing or being fatally undermined.

In addition, thinking about privacy in terms of informational self-determination and attempting to shift current political and legal debates such that the onus is on the state to better justify the expansion of security-related surveillance powers may have other benefits that go beyond bolstering existing individual privacy protections. Closely related to the idea of informational self-determination is the notion that it is possible to own information about oneself, and as such one of the arguments in favour of the new right is that it may open the door to broader discussions about the possible economic value of privacy.

At present, we assume that once an individual (either willingly or unwillingly) reveals information about him- or herself, that individual's interest in and claim over that information is substantially weakened. He or she may attempt to prevent others from receiving that information or to stop it from being used by certain organisations,

but there is no suggestion that such assertions of control are based on clear ownership or concepts of property. If, however, someone who possessed or used information about another individual were required to financially compensate that person—that is, required to pay for the privilege of required to pay for the privilege of using someone else's personal information and asserting a form of control over it—then it is possible that the use of categorical identities and certain types of surveillance and data matching would naturally be constrained.[66] Governments and organisations would, it seems reasonable to assume, think twice about acquiring information or sharing it if, in just the same way copyright royalties are paid to artists, they may also have to pay the individuals to whom the information pertains.

Although such a market in personal information may be no more likely to come into being than Brin's 'transparent society', thinking about the applications and limits of the right to informational self-determination along these lines does provide the basis for the formulation/conception/conceptualisation of new ways of both resisting the imposition of categorical identities and reasserting the collective and individual interest in privacy.

CONCLUSION

In this chapter, an attempt has been made to show how the pursuit of security and the continued expansion in state surveillance affect privacy and identity. Although it is clear that legislation such as the Anti-terrorism Act and the PATRIOT Act represents a threat to many well-established human rights—such as the right to silence and the

[66] I am indebted to Kevin Haggerty for first raising the question of a potential market in personal information, and for providing various insights into the implications for privacy and surveillance of making users of that information pay for it. It is an intriguing and powerful idea that I hope he will take up in print.

right to a fair trial—there is a danger that because liberals and civil libertarians continue to focus much of their attention on the threat to these fundamental civil liberties, we risk losing sight of the fact that many other less well-defined but no less important rights—including, namely, privacy—are being gradually worn away. Furthermore, it is important to acknowledge that although the events of September 11 were enormously significant in terms of shifting the balance in the security–rights debate, many of the threats to individual freedom and autonomy that now appear so clearly have in fact been present for a very long time.

Security, surveillance, identity and privacy are intimately connected. As states attempt to increase their ability to defend their citizens from external and internal threats, they also necessarily risk undermining the ability of the individuals within their borders to live free from scrutiny, suspicion, categorisation and discrimination. Many existing privacy protections are incapable of addressing the underlying challenges posed by the pursuit of security because they were developed during a time in which the distinction between the public and private was much clearer than it is today, and because the costs of acquiring, processing and sharing information were once much higher than they are today. If we are to maintain some degree of control about the way in which our identities are constructed and used, it is essential not only to begin to think about what identity and privacy mean, but also to take positive steps to develop legal and other means of resisting state demands to submit to categorisation and control. Unless we do so, regardless of whether we are more secure from physical threats, we may end up surrendering our identities—and in the process, surrender a part of ourselves.

REFERENCES

Alderman, E and Kennedy, C, *The Right to Privacy* (New York, Knopf, 1995).

Anderson, C, 'The Zen of Jeff Bezos', *Wired Magazine*, January 2005, available at http://www.wired.com/wired/archive/13.01/bezos.html (accessed 31 September 2006).

Baer, S, 'Broader US Spy Initiative Debated; Poindexter leads Project to Assess Electronic Data, Detect Possible Terrorists; Civil Liberties Concerns Raised', *Baltimore Sun*, 5 January 2003.

Calhoun, CJ, *Critical Social Theory: Culture, History, and the Challenge of Difference* (Oxford, Blackwells, 1995).

Dauenhauer, B, 'Paul Ricoeur' in EN Zalta (ed), *The Stanford Encyclopedia of Philosophy*, Winter 2005 edn, available at http://plato.stanford.edu/archives/win2005/entries/ricoeur (accessed 11 December 2006).

Davies, S, *Big Brother: Britain's Web of Surveillance and the New Technological Order* (London, Pan Books, 1996).

DeCew, J, 'Privacy' in EN Zalta (ed), *The Stanford Encyclopedia of Philosophy*, Fall 2006 edn, available at http://plato.stanford.edu/archives/fall2006/entries/privacy (accessed 11 December 2006).

—— *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology* (Ithaca, Cornell University Press, 1997).

Deleuze, G, 'Postscript on the Societies of Control' (1992) 59 *October* 3.

Doyle, C, 'USA Patriot Act: A Sketch', (Congressional Research Service report RS21203 for Congress, 2005).

—— 'USA Patriot Act Sunset: A Sketch' (Congressional Research Service report RS21704 for Congress, 2005).

Dworkin, R, *Taking Rights Seriously* (London, Duckworth, 1977).

Egger, SA, *Serial Murder: An Elusive Phenomenon* (Westport, CT, Praeger, 1990).

—— 'A Working Definition of Serial Murder and the Reduction of Linkage Blindness' (1984) 12 *Journal of Police Science and Administration* 348–57.

Feldman, D, 'Privacy-related Rights and their Social Value' in P Birks (ed), *Privacy and Loyalty* (Oxford, Clarendon Press, 1997).

—— 'Secrecy, Dignity or Autonomy? Views of Privacy as a Civil Liberty' (1994) 47(2) *Current Legal Problems* 41.

Franko Aas, K, 'From Narrative to Database: Technological Change and Penal Culture' (2004) 6(4) *Punishment and Society* 386.

Fried, C, *An Anatomy of Values* (Cambridge, Harvard University Press, 1970).

Galison, P and Minow, M, 'Our Privacy, Ourselves in the Age of Technological Intrusions' in R Ashby Wilson, *Human Rights in the 'War on Terror'* (Cambridge, Cambridge University Press, 2005).

Garland, D, *The Culture of Control* (Oxford, Oxford University Press, 2001).

Gene Watch UK, *The Police National DNA Database: Balancing Crime Detection, Human Rights and Privacy* (Buxton, GeneWatch UK, 2005).

Gilliom, J, 'Struggling with Surveillance: Resistance, Consciousness and Identity' in K Haggerty and R Ericson (eds), *The New Politics of Surveillance and Visibility* (Toronto, University of Toronto Press, 2006) 111–40.

Goold, B, 'Open to All? Regulating Open Street CCTV and the Case for "Symetrical Surveillance"' (2006) 25(1) *Criminal Justice Ethics* 3–17.

Higgs, E, 'The Rise of the Information State: The Development of Central State Surveillance of the Citizen in England, 1500–2000' (2001) 14(2) *Journal of Historical Sociology* 175–97.

Inness, J, *Privacy, Intimacy and Isolation* (Oxford, Oxford University Press, 1992).

Levi, M and Wall, DS, 'Technologies, Security, and Privacy in the Post-September 11 European Information Society' (2004) 31(2) *Journal of Law and Society* 203.

Lustgarten, L and Leigh, I, *In from the Cold: National Security and Parliamentary Democracy* (Oxford, Clarendon Press, 1994).

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

—— 'Surveillance Studies: Understanding Visibility, Mobility and the Phenetic Fix' (2003) 1(1) *Surveillance and Society* 3.

McCartney, C 'Forensic DNA Sampling and the England and Wales National DNA Database: A Sceptical Approach' (2004) 12 *Critical Criminology* 157–78.

Narr, W-D, 'Wir Bürger als Sicherheitsrisiko: Rückblick und Ausblick' (1998) 60 *Bürgerrechte & Polizei/CILIP* 30–40, available at http://www.cilip.de/ausgabe/60/narr60.htm (accessed 31 September 2006).

Nissenbaum, H, 'Privacy as Contextual Integrity' (2004) 79(1) *Washington Law Review* 101–39.

Norris, C, 'Algorithmic Ssurveillance' (1995) 20 *Criminal Justice Matters* 7–8.

Norris, C, Moran, J and Armstrong, G, 'Algorithmic Surveillance: The Future of Automated Visual Surveillance' in C Norris, J Moran and G Armstrong (eds), *Surveillance, Closed Circuit Television and Social Control* (Ashgate, Aldershot, 1998) 255–76.

Parent, W, 'Privacy, Autonomy, and Self-Concept' (1983) 24 *American Philosophical Quarterly* 81–89.

—— 'Privacy, Morality and the Law' (1983) 12(4) *Philosophy and Public Affairs* 269–88.

Phillips, D, 'Privacy, Surveillance, or Visibility: New Information Environments in the Light of Queer Theory', Paper presented at the annual meeting of the International Communication Association, New York City, available at http://www.allacademic.com/meta/p12412_index.html (accessed 11 December 2006).

Privacy International, 'Increased Abuse of Data and Disregard for Protections', press statement, 9 August 2004, available at http://www.privacyinternational.org (accessed 31 September 2006).

—— 'Terrorism Profile: US' (3 October 2005), available at http://www.privacyinternational.org (accessed 31 September 2006).

Pütter, N et al, 'Bekämpfungs-Recht und Rechtsstaat. Vorwärtsverrechtlichung in gebremsten Bahnen?' (2005) 82 *Bürgerrechte & Polizei/CILIP* 6–15; Kutscha, M, 'Auf dem Weg zu einem Polizeistaat neuen Typs? (2001) *Blätter für deutsche und internationale Politik* 214–21, available at http://www.blaetter-online.de/archiv.php?jahr=2001&ausgabe=02 (accessed 4 December 2006).

Ricoeur, P, 'Reflections on a New Ethos for Europe' (1995) 21(5) *Philosophy and Social Criticism* 6.

Roggan, F, *Auf dem legalen Weg in einen Polizeistaat. Entwicklung des Rechts der Inneren Sicherheit* (Bonn, Pahl-Rugenstein, 2000).

Rose, N, *Powers of Freedom: Reframing Political Thought* (Cambridge, Cambridge University Press, 1999).

Scanlon, T, 'Thomson on Privacy' (1975) 4 *Philosophy and Public Affairs* 315–22.

Schoeman, F, 'Gossip and Privacy' in RF Goodman and A Ben-Ze'ev (eds), *Good Gossip* (Lawrence, University Press of Kansas, 1994).

Stanley, J and Steinhardt, B, 'Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society' (ACLU Technology and Liberty Program, 2003).

Tempest, M, 'Britain Facing "Most Sustained Threat since WWII" says Reid', *The Guardian*, 9 August 2006, available at http://politics.guardian.co.uk/terrorism/story/0,,1840482,00.html (accessed 31 September 2006).

Thomson, J, 'The Right to Privacy' (1975) 4 *Philosophy and Public Affairs* 295–314.

Torpey, JC, *The Invention of the Passport: Surveillance, Citizenship and the State* (Cambridge, Cambridge University Press, 2000).

Westin, A, *Privacy and Freedom* (New York, Atheneum, 1967).

Williams, R, Johnson, P and Martin, P, 'Genetic Information and Crime Investigation' (University of Durham School of Applied Social Sciences, report, 2004).