Chapter 7

Privacy as currency: crime, information and control in cyberspace

Stéphane Leman-Langlois

Introduction

Contemporary debates over the nature or extent of a 'right to privacy' are usually conducted at the level of politics, ethics and jurisprudence and have thus ignored a fundamental new development: the idea of privacy as a principle or *right* has been rendered moot by a number of new practical realities. The most important development is that privacy, or the information that constitutes it, has been transformed into an exchangeable currency. It is no longer a right in the classical sense of the word, where it served as a definition of the limits of the controlling power of the state; instead, it has become an adjustable quantity with different relative values for individuals, states and private enterprises. It may be exchanged for services, goods, personal safety, convenience or ease of use of existing services and goods. The citizen-consumer now has a quantity of 'disposable privacy' or 'privacy capital' that may be bartered for access to computer services, software or individual police protection; for the more rapid payment of welfare cheques or tax returns; to obtain new goods and services – air travel tickets, mortgage rates, motorcars, etc. – at lower prices; or for access to the virtual and physical premises where such services and goods can be obtained.

Further, in spite of the nearly exclusive focus on state action in contemporary literature about privacy, in reality privacy is no longer solely threatened by the state's ability to gather, store, analyse, disseminate and use information about its citizens. For instance, the dominant discourse on privacy focuses on the threat represented

by closed-circuit television (CCTV) and, almost invariably, on *public* cameras – ignoring the thousands of privately owned cameras that surround the few installed by the police. In late-modern neoliberal times and the risk/information society, this 'Big Brother' understanding of threats to privacy has become obsolete. But, more importantly, this chapter suggests that the *meaning* of privacy has drifted away from a central concern with visibility and knowledge.

This chapter concentrates on cyberspace as a site for information exchange and, more specifically, on the open, industrial or commercial cyberspace where citizens, subjects or consumers converge in various types of activities, from banking to shopping to playing MMOGs (massively multi-player online games). Of course, many other forms of information collection and communication exist elsewhere – cyberspace itself is much, much broader than the limited set of activities most of us engage in online. Since it is the social meaning of privacy and personal information that is of interest here, I concentrate on areas where the individual is (relatively) aware of the nature of the information exchanged and of the entities involved.

Before we proceed, I should emphasize that privacy has always had many meanings, which tend to vary between authors, perspectives and contexts. Five different common conceptions of the term 'privacy' relevant to cyberspace behaviour are as follows:

- *Control over information*: assurance that personal information will be used according to contractual arrangements.
- *Secrecy of information*: ability to escape surveillance or to protect against unwanted prying; access to anonymity.
- *Desire to protect personal space*: psychological need to retreat to non-social space, to engage in individual activities.
- *Right to keep secrets*: rules defining institutional, social, political or administrative limits to collecting and sharing information.
- *Data security*: IT system safeguards against unauthorized access to protected information.

The first common use of the term 'privacy' is frequently found in end-user licence agreements (EULAs), where software vendors offer their clients varying degrees of assurance that any information provided to them will (within specified limits) serve only purposes agreed to by the parties. The same form of privacy is also offered by consumer loyalty programmes that collect data on consumer behaviour in exchange for special benefits ('air miles' or more prosaic 'points,' etc.). The second use relates to one's ability to keep secrets

from various potentially interested parties, especially the state. This is closely related to our ability to remain anonymous, something made possible by modern urbanization – personal secrets were few and short-lived in smaller, close-knit communities. Paradoxically, this urban anonymity seems to have led to new desires to confess publicly even the most embarrassing secrets, whether on Internet forums or on 'reality' TV shows. (Although only a few are actually chosen to participate, great numbers of hopefuls invariably crowd early auditions.) The third common meaning of privacy is based on the purported existence of a fundamental human need to be alone, to retreat from constant social gaze or interaction. In fourth place is the normative, rule-based conception of privacy as a right, which gives rise to a set of regulations designed to protect it. This definition of privacy is usually presented as an element of a zero-sum game of power, where adding information on one side of the scale automatically lightens the other side. Finally, in the context of securing IT networks, privacy is conceived of as the implementation of effective technical barriers to illegitimate (ethics level), unapproved (administrative level) or unlawful (legal level) data access.

Some of these definitions rest on metaphysical absolutes; others imply undefined states of mind (desires, bio-psychological tendencies, calculations, etc.); and still others are insufficiently specified (measuring information secrecy requires evaluating the availability of all of one's personal information; since this cannot be done in practice, the level of secrecy can only be speculative).

For the specific purposes of this analysis, I define privacy as the total of all forms of personal information about an individual – whether or not such information is recognized as 'private' by its object/source or by its repository – that may be communicated (given, bought or otherwise transferred). This definition has the advantage of taking into account the many kinds of information that are not part of the traditional, and overly subjective, understanding of privacy as one's 'private affairs', as elements of knowledge that are held by their originator to be secret or to have limited distribution. Instead, it is a purely quantitative notion of privacy meant to circumvent the usual normative, technological or psychological pitfalls. My discussion of privacy covers a great deal of ground and includes habits, grocery lists, whereabouts, music preferences and all other forms of knowledge that can be formulated and compiled about a person. This comprehensiveness is important since, in the era of behavioural analysis and data mining, a surprisingly complete personal portrait can be produced from apparently insignificant titbits.

In late-modern society, this information – and other types we have yet to imagine – is disseminated over a dynamic web composed of a multitude of very different entities. The state and its various institutions are among these entities but, although still powerfully determinant through various forms of regulation and production, it no longer holds a monopoly in this matter. For the most part, information is collected, analysed, diffused and archived by non-state actors whose mission is to maximize the efficiency of many aspects of industrial production, distribution and consumption.

This chapter is organized into three main parts. First, I review the key social, demographic, economic and political factors that form the contingent context where our perception of privacy evolves. The second section analyses the most important modes of information exchange in cyberspace in order to reconstruct the main practical aspects of computerized privacy. The last section explores the function of personal information in the computer user's everyday experience of cyberspace. We see that shared private information does not accumulate in secrets vaults or give rise to totalitarian, clandestine police action (though it also does): rather, it structures our experience of cyberspace.

Late-modern society: consumers, risks, information ~ and markets

Four dominant features of late-modern society interact to produce the social environment that transforms privacy, defined as personal information, into currency.

Consumers

The first feature is consumerism – the way we approach both the goods and services we desire and the means we use to obtain them. In a cash society, we fulfil our needs and desires through the use of legal currency: such currency has a limited, physically set value (but no intrinsic value, of course). It is owner neutral, immediately bearer usable and requires no interaction between the user and the issuer/guarantor (the state). In contemporary society, the use of this 'pure' exchange vector is on the decline. Most other forms of payment (cheques, but more importantly credit cards, debit cards and other like methods) are services that must be acquired by the user. They have stricter usage rules, necessitate a constant exchange

of information between the issuer, the user and the vendor, and require financial compensation, etc. In non-physical cyberspace, these are the only accepted means of payment. (One has to be careful not to overstate the importance of e-commerce, since at present it is only a small proportion of total consumption.)

Consumer society, as Baudrillard noted (1970), is a culture founded on need rather than on promised abundance. Since goods and services are plentiful, few of us go hungry or have no roof over our heads, and most of us manage to fulfil quite a few of our decidedly superfluous desires. The consumer's subjective experience of reality is, however, of constant need, not of satisfaction – a continuing subjective impression of un-satisfaction that is fundamental to the production cycle. Any satisfaction must be fleeting, evaporating under the pressure of technological obsolescence and massive advertising, replaced by an insatiable desire for novelty and accumulation. This urge for the new applies not only to the goods and services we 'need' but also to the financial services we use to acquire them. Since the 1970s, credit cards have largely overtaken cash as the main form of payment. The seductive power of easily available credit services has created ever-increasing levels of debt and personal bankruptcy, as well as the lowest savings rate in history. (The other record low occurred during the great depression.) The Internet consumer is immersed in an intensive, continuous flow of information about desirable products and easy payment.

Risks

Ulrich Beck introduced a remarkably fertile concept in 1992 with his work on risk. While his primary focal points were the new risks produced by technology, specifically those associated with nuclear power and pollution, the idea of risk was quickly adapted to the study of multiple social phenomena, particularly crime and terrorism. Security experts define risk as a combination of likelihood and the potential severity of the effect, or 'criticality.' Whether a type of crime or terrorism is more 'risky' today than it was 30 years ago has become less important than the fact that such activities have now been reduced to their risk content – they now *are* risks. In Canada, one of the main post-9/11 changes in government was the creation of what is essentially a department of risk management, named 'Public Safety Canada' (PS). To PS, epidemics, destructive weather, industrial espionage, crime, terrorism and threats to computer security are all primarily risks and can all be managed centrally through a unified model (with different responses, of course).

In a risk society, criminal activity is not seen as evil, pathological or even illegal. Instead, it is one of many different risk factors that one should be informed about in order to take the proper steps to avoid or at least manage it (for instance, through insurance or by adopting safer behaviours). A risk-based understanding of crime is uninterested in matters of aetiology, rehabilitation or rights (whether the victims' or the offenders') but only in actuarial assessment and classification according to probability and criticality (Feeley and Simon 1992; O'Malley 1998 2004).

One form of technology whose risks Beck paid far less attention to is IT, now at the forefront of media and government attention. We are constantly bombarded with information about formless, generalized IT risks: viruses, identity theft, paedophiles looking for our children on the Internet, black-hat hackers bent on turning our home computers into bots, terrorists destroying the power distribution infrastructure, etc. There are also periodic scares such as the infamous 'Y2K' bug (planes were predicted to fall from the sky), the 2000 warning from Richard Clarke (former White House National Security Council adviser) about an upcoming 'Digital Pearl Harbour' or the 2004 Microsoft 'JPEG' vulnerability/virus. As with risks linked to conventional criminality, we are asked to take action to manage our risks better: we are given information about risks, risk mitigation strategies are suggested (better password management, parental supervision, etc.) and we are drafted as civilian guardians of the net with such programs as 'CyberTip.ca', which encourage the reporting of the sexual exploitation of children on the Internet.

Information

Logically, risk assessment demands sufficient, timely, relevant information; the more information, the better the assessment. That the development of the risk society has coincided with increasing concern about the validity, quantity and flow of information is not fortuitous. Whether or not we take part in the 'information society', industries related to the production, treatment and transfer of information (entertainment, Internet, IT) are in a period of exponential growth. Since the 1990s and the invention (and subsequent disappearance) of the catch phrase 'information superhighway', governments have been increasingly concerned with the many aspects of the concepts of 'information society', 'information revolution', and 'knowledge economy', especially as they effect education, governance and industry. There are important social and political consequences to the use of

these 'information society' concepts. For instance, they tend to increase important social and economic differences and grossly unequal access to information. They further obscure demographic, political and social areas where information is less abundant (see Mattelart 2001). They also legitimate the increasingly strict and powerful protection of 'information industries' and so-called 'intellectual property' (which, paradoxically, *disrupts* the flow of knowledge). Examples include the recording industry's all-out war against file sharers (Leman-Langlois 2003 2006) or the motion picture industry's success at criminalizing the unauthorized recording of new releases in theatres and, of course, the creation of entirely new forms of 'crime', such as the 'attempted copyright infringement' in the US House Intellectual Property Bill 2007 (Ars Technica 2007). These very different phenomena point to one important development: information is, more than ever, a *product*, conceptually separate from other goods and services.

Just as with risk, this conclusion should not be taken as a claim that we are more or better informed than we were in the previous 'non-information' society, or that information makes us better or more productive individuals (Garnham 2000). Information can be false, erroneous, misleading, incomplete, contradictory or just plain confusing, and adding more of it does not necessarily solve these problems – it may actually exacerbate most of them. What is important is the new economic and political power generated by the production and exchange of information.

As well, as we see in a moment, information gives birth to new worlds where individuals can lead increasingly diverse and varied lives.

Markets

The changes discussed above are taking place in neoliberal times, where power structures are exploding away from the state and towards multiple other institutions: commercial, private, individual, communitarian, professional, corporate, supra-national, etc. Concurrent state disinvestment and deregulation have greatly enhanced the social power of most industrial markets. Though conventional policing remains, and is likely to remain a state function in the future (the growth of private policing remains essentially a North American phenomenon), cyberpolicing is overwhelmingly private. It is deeply enmeshed with the data surveillance inherent to any online activity. While some private actors are more than happy to call on 'the system' when it seems financially expedient (see Chapter 5, this volume),

cyberspace is still 'lawless' space, in the sense that the public police remain nearly invisible – a state of affairs unlikely to change soon (see Chapter 6, this volume).

The state used to be the sole subject of any analysis of privacy, surveillance or the collection of personal files. Dystopian fictions (*1984*) and realities (the Stasi files) also put the state apparatus in the middle of all control structures. Recently, many authors note that the actual power of the state appears to be in relative decline in most contemporary societies (for instance, Wood 2004). This decline has been interpreted as an indication that Foucault's (1975) use of Bentham's 'panopticon' as a metaphor for surveillance, since it rests in part on the centralization of surveillance, no longer applies (Haggerty 2006; Dupont forthcoming). This seems only more so in cyberspace, where the state is far less visible and has no tradition of legitimacy. The idea that surveillance is antagonistic by nature is also outdated. On the other hand, the state's actual impact notwithstanding, evidence shows that behavioural change is still the main objective of surveillance, whether consensual or not, and the *object* of surveillance, the modern, 'rational' human capable of self-discipline, is also the same. The difference is that now conduct is changed not by the threat of punishment but by the promise of reward.

The industrial information exchange

Needless to say, immense amounts of information about citizens are being collected, analysed and acted upon in complete secrecy by the state, private enterprises and other citizens (Brodeur and Leman-Langlois 2006). In cyberspace, however, individuals also knowingly provide access to vast amounts of personal information. They also do it over the phone or in person, of course, but cyberspace seems many orders of magnitude ahead. Lyon (2006: 8) refers to this phenomenon as the 'panopticommodity,' a world of surveillance in which the surveilled actively participate in revealing themselves and providing information about their physical characteristics, habits and preferences because doing so entitles them to various benefits. Whitaker's (1999) 'participatory panopticon' points out that globalized surveillance rests on what Foucault would deem 'positive power' – power derived through a reconstruction of consent. In this brave new world, the end of privacy is not the result of the actions of ill-intentioned or ill-advised entities: it occurs because we no longer value it.

Most authors see the disappearance or reduction of privacy as a modern social problem. Whitaker, for instance, warns of dire consequences, such as the destruction of social solidarity, the (further) disempowerment of the have-not classes and the exclusion of dissenters. As Mathiesen (1997) has already noted, the surveillance tools now available to the masses, rather than working to counter such problems, instead produce ever more frivolous, inconsequential gossip rather than useful information. Other analysts approach all technologies as intrinsically suspect and destined to augment the speed and intensity with which totalitarian practices are introduced (Mattelart 2001; Fischer 2006; Los 2006). Technologies that appear to invade a sacrosanct inner personal sphere in order to extract information are deserving of special scorn. The opposite extreme is to see technology as an answer to all modern political and social problems. Etzioni (1999: 2), for instance, presents a series of straw-man arguments ('to begin a new dialogue about privacy, I have asked … if they would like to know whether the person entrusted with their child care is a convicted molester') that suggest that all privacy 'problems' can be solved with technology. Data mining and the automated computer analysis of information have also been presented as ways to protect privacy since no humans are used to pry into the personal affairs of the targets (Brodeur and Leman-Langlois 2006).

One extremely important aspect of information exchange is that a large proportion of the supposedly privacy-reducing technologies is being adopted not by governments or large corporations but by individual consumers who find them useful tools of social networking, communication, entertainment, etc. The argument that these users are unaware of the 'bad' side of the tools they use is becoming extremely thin and requires the assumption that a majority of the public is technologically ignorant. This ignorance hypothesis is essentially a normative argument based on the idea that important, significant or dangerous truths are being forgotten by citizens. It is true, of course, that the general public, and especially the so-called 'Internet generation', is far less techno-savvy than one might imagine. For instance, many university students are incapable of efficiently searching the Internet and are forced to use prepackaged, easy-access, mass-market information. However, the assumption that they are giving away privacy information because they do not see its 'true' value simply does not fit the facts. On the contrary, they have learnt that all information has a *market* value.

Cyberspace encompasses a broad range of activities involving information exchanges between individuals and various entities, and the nature, purpose and beneficiaries of the gathered data can differ widely. It is useful to break this vast range of activities into a few discrete, yet overlapping categories.

Virtual payment

As many have already pointed out, there are instances where we agree to provide information about ourselves in order to pay for goods, services and information that we want. The most common example is the use of credit cards (issued by banks or large retailers) or other forms of mediated payment, such as PayPal. These are not specific to cyberspace but cyberspace consumers, unlike 'meat space' consumers, cannot choose to pay in cash. Even bartering, on the Internet, leaves clear traces that have no equivalent in the physical world.

Users may not know exactly how much information is being recorded, how long it will be kept, to what extent sophisticated analysis techniques will add value to it (building consumer profiles, sharing credit histories with multiple other entities through Equifax, Experian and Transunion) or who may have access to it now or in the future. However, receiving a statement every month certainly indicates that one's purchases have been recorded. Various messages also hint that spending and reimbursement habits have been analysed, such as periodic rises in the allowed credit limit. (Conversely – or perhaps consequently – we may receive a message informing us that the normally required minimum payment has been suspended to 'help with unforeseen financial demands'. Interest costs continue to apply, of course.)

Unsurprisingly, in view of the enormous possible losses, the misuse of this type of personal information by third parties (such as so-called identity theft) is making the public increasingly wary and is one of the main problems limiting the growth of Internet commerce (Conference Board 2005). Consequently, the continuous analysis of spending habits has been introduced to identify 'abnormal' uses of credit cards, which are statistically associated with illegitimate use. Card holders who depart from their usual routines may get a phone call from the card issuer's offices to confirm that they have made the purchases being credited to the card.

Rewarding loyalty

Loyalty programmes are different in a key respect: the recording of one's purchases is not logically implied in their use. However, the literature included when someone joins, as well as information on corporate websites and in other publications, clearly states that information is collected, though it is often less clear about the intended uses of that information or who its beneficiaries are. Loyalty Group (2007) mentions that it collects information:

> to ensure the proper functioning of the AIR MILES® Reward Program; to meet the direct marketing, product development and research requirements of the AIR MILES® Reward Program and its participating Sponsors; and to improve the promotional offers and services of the AIR MILES® Reward Program and its participating Sponsors.

It is less explicit about the nature of the information being collected. For example, there is no mention of whether individual line items or only total purchases are recorded, whether the record is time stamped, whether mode of payment is noted, etc.

Third-party loyalty programmes, such as Air Miles, are most useful for conventional marketing, outside cyberspace, because they are actually subcontractors for the task of database management, which small and medium retailers might find onerous (leading them to revert to the classic cardboard fidelity card). By contrast, Internet retailers can create their own automated loyalty programmes easily and can start collecting visitor information right away, since their entire operation is already database dependent. Cyberconsumers are also often asked to create personal profiles where even more information about them is collected.

The user-friendly cyberspace

Amazon has one of the most sophisticated systems for collecting and using information about its customers, as well as visitors. In addition to defined personal data, it asks them to make recommendations and to identify the books they already own. The reward for this is, however, slightly different: participation creates a corner-bookstore, wave-to-the-owner feel for the colossal retail warehouse, making it a cosy, user-friendly space.

While it is true, in theory, that the Internet has given any individual user the capacity to 'publish' information and, conversely, to find

millions of various sources of information, in reality this glut of data has created a need for simplification and streamlining. In fact, to a large extent the very creation of the World Wide Web was in part the application of a varnish of simplicity to the chaotic, infinite net of information (which has grown a thousand-fold since). Early on, Internet portals were introduced to provide further streamlining, offering a one-stop, pre-digested, standardized and easy-to-use library of selected sources of information (selected in part in terms of the portal owner's business ties to content providers).

Today, portals have grown to include just about any form of service in cyberspace. Microsoft's MSN is the most accomplished example of a multinational, multi-service portal where users can chat, read news (from MSNBC), manage their agendas, access videos, purchase music, books and airline tickets, find a date, consult an encyclopaedia (Microsoft's *Encarta*, of course) and much more. Portals from many other Internet service providers (ISPs) – for instance, Canada's Bell Sympatico's, the largest ISP in Canada – are in fact MSN clones. Microsoft has devised a uniform password system for all its member portals, sites and subsites called 'Windows Live ID' (originally, '.NET Passport') aimed at reducing the number of passwords users must remember to surf from one personalized service to the next. It also allows the creation of a centralized database of user behaviour.

Most major portals include a customization function where users can change the 'look and feel' of the interface and can select content categories according to their personal preferences, etc. (thus enabling 'My MSN', 'My AOL', 'My Yahoo,' and so on). In most cases these preferences, as well as the user's behaviour within the portal, are recorded and analysed in order to tailor the content offered to the user's inferred 'tastes'. This also applies to advertisements placed on each new page consulted. Search engines such as Google, Yahoo or Ask Jeeves also try to make the Internet user's experience as personalized, and as simple, as possible by offering a variety of customization options. Amazon and other retailers with vast inventories have similar problems. Their interfaces often look like those of search engines and could leave users with nothing to help them find their way through thousands of choices. Amazon tries to counter this through book suggestions based on customer behaviour while browsing and purchasing items. (These suggestions also take into account the retailer's marketing strategy and current inventory.)

In all cases, most of these functions rely on cookies left on the user's computer, which serve to track behaviours and preferences and to link users to their profile on the site's database. Most commercial

and government websites (except in the USA, where government websites are forbidden by law to use cookies or other types of tracking devices) install multiple cookies (27 per cent of all individual servers link to cookies; Security Space 2007). Cookies became the target of much scorn when consumer and privacy advocates learnt of their presence and function. To a large extent the concerns, and certainly the panic, were clearly exaggerated: in reality cookies are essentially harmless. Yet alternative browsers were quick to respond to the wave of concern and offered users the open management of cookies and the ability to refuse them in bulk or to chose among them. Eventually Microsoft's Internet Explorer, dominant in the market (82 per cent) because of its automatic presence in Microsoft's operating systems (since Windows 95), began to provide this service as well. However, most internet users remain entirely oblivious to cookies. What is more interesting, most (76 per cent) of those who are fully aware of their function choose to accept them in bulk anyway (Pew Internet 2000). While there are no recent numbers, this does not invalidate the point. The problem is, of course, that the selective management of cookies severely degrades one's experience of cyberspace, since multiple message boxes constantly appear on the screen to prompt users to exercise their freedom to accept or reject each cookie. Bulk refusal or deletion has an equivalent effect: any customization, automatic user recognition and preselected content vanish, and many websites will simply refuse to display any content at all (especially online merchants and financial institutions).

Finally, cyberspace is mediated by an array of applications that must be installed on individual computers. Most of these applications require information in order to work properly and may gather it any of three main ways. First, many software packages demand, or at least suggest, that the user 'register' their copy. This registration process usually involves communicating personal information. In most cases registration is elective but rewarded by special promotions, services or various gadgets. Secondly, it is not uncommon for programs to monitor the way they are used and to send that information back to their distributor. Popular music management packages routinely gather anonymous statistics (for instance, AOL's WinAmp, Real Networks' RealPlayer or Apple's leading iTunes/QuickTime). Users are informed of this in more or less explicit terms, sometimes deep into the scroll-down message box where they must click to agree to licence terms – Apple's iTunes/QuickTime EULA clearly states that computer state and usage information will be sent to Apple and its partners, but the agreement is a rebarbative 4,000 words long. Of

course, some applications collect and report information without telling the user – using so-called 'spyware,' which is beyond the scope of this chapter. Finally, software that has communication as its primary function obviously requires geographic or electronic identification co-ordinates in order to perform its function. Web browsers, at the minimum, give out Internet protocol addresses and various types of information about the computer's ability to reconstruct the pages requested by the user (browser type, operating system and so on). Other cyberspace communication tools, such as commercial Voip or Skype, AIM, ICQ or MSN, are also dependent on personal information. While tools that provide anonymity are available for simple web surfing, they would entirely defeat the purpose of the applications in this third category.

Showing oneself

The new catch phrase is 'Web 2.0.' Under this umbrella, analysts refer to any and all cyberspace applications that invite users to participate in their content, appearance or functionality. The aforementioned glut of information in cyberspace, the virtual infinity of its depth, means that individual websites are no longer efficient means of communication. There are exceptions, of course, but, by and large, independent personal websites are doomed to oblivion. Instead of building a personal website likely to become a molecule in an ocean of other such sites, Web 2.0 users actively participate in hugely popular sites. Wikis are built on this principle.

In Web 2.0, a sizeable proportion of netizens engage in behaviours with the *purpose* of letting third parties watch (some of the) activities they engage in, for either exhibitionist pleasure, personal pride or communication. All three motivations are apparent on social networking sites such as MySpace, FaceBook or the newer Widows LiveSpace, where technology is used to create friendship rings among individuals sharing like interests. In order for the concept to work, participants must list their interests, preferences, the place where they live, what they do for a living, their social status, etc. So far it seems to be a success: more than half of all teen netizens have created a personal profile on one or more social networking sites (Pew Internet 2007). The extent to which this creates an entirely new conceptualization of friendship and a new, more streamlined, efficiency- (robot-) driven social life will be debated for years to come. However, MySpace offers an interesting sociological 'site' where individual users can be observed managing their personal

information and making choices between what is private and what is not. The most obvious observation is that the position, movability and porosity of the line between private and public are, literally, *infinitely variable* and, consequently, that no codification is possible.

Constructing the commercial cyberspace

Each of the aspects of information exchange listed above involves a specific conception of individual agency and purposes online. Cyberspace appears as a space of consumption, where individuals are eager to exchange various forms of payment for various goods, services and information. In that structure, personal information, including personal data (such as occupation, gender, credit card numbers, age, etc.) as well as accumulated facts about current behaviour, whereabouts, friends, etc., is property and has a variable exchange value. Privacy has therefore lost its old classical core; it is no longer conceivable in terms of a protected, secret, inner personal space filled with inherently 'private' information – information given an objective quality of intimacy. We have already briefly touched on the multiple rewards offered to those who share information about themselves. In the next section I explore further the matter of context and what we might call 'flexible space.'

Flexible space

Personal information modifies the structure, content and interactions possible in the cyberworld. This has little impact on those of us who read emails once a week or find phone numbers on Internet listings. However, there is a minority, and a growing one, of citizens who spend increasing amounts of their time on web-mediated activities of infinite forms. In these cases, we might categorize the reality-altering effects of the information exchange under two main headings.

Reflexive space

We might consider, for the moment, that the most advanced form of flexible space is what visitors will find at Linden Lab's Second Life (another is Makena Technology's There). Currently this is the most technologically advanced form of social networking, where users move through space as disincarnate floating points of view, presenting themselves to others as 'avatars' modified to their fancy. This form of cyberworld existence and interaction is quite familiar to those

who have played computer or console third-person games. Yet two differences are immediately evident. First, the world is a continuous creation of other inhabitants – it is Web 2.0 at its current maximum. Secondly, the main object of the experience is communication and other forms of interaction with others – though, of course, few present themselves in Second Life as realistic facsimiles of their 'true self' (let us forget for a moment the sociological Gordian knot hidden behind this concept). Of course, online or local multiplayer games have had this type of social interaction feature for years, especially role-playing games. Many also allowed players to build their own 'maps' where capture-the-flag or 'deathmatch' games could take place. Yet Second Life, though derived from those concepts and technologies, is explicitly geared towards recreating a realistic, *ordinary* world where only some well circumscribed flights of fancy may take place. Deviance, crime, the misuse of software, the harassment of other citizens, etc. are punished and noted in the daily 'police blotter' on the main site (Second Life 2007; for more on crime in Second Life, see Chapter 6, this volume). Of course, one of the most important aspect of life in Second Life is continuous, microscopic surveillance and the collection of all and any information generated by actions taken by visitors.

One area where Second Life connects to physical space is money. The cyberworld's economy is booming, and the local currency ('Linden dollars') may be exchanged for any other currency – and all gains are tax free. The border between Second Life and 'real' life is clearly visible but effortlessly crossed. Continuing advances in technology will no doubt tend towards the greater integration of cyberspace with physical space. Neural activity sensors (see http://www.emotiv.com/2_0/2_1.htm) and semi-transparent eyeglasses will permit seamless integration and interaction with both the physically present and the 'avatars' (some of which will be machines) and other cyber-objects, in what is referred to as 'augmented reality'.

Augmented reality is not quite around the corner, and examples of flexible space that can be found today are less spectacular. However, they do offer a glimpse into the future, especially the evolution of such concepts as privacy and personal information. For the time being, paying sponsors can already update the way various objects look in game cyberworlds, whether the game is played on a remote server or on the user's own computer or game console. Limited at first to putting advertising hoardings in the environment, they can now remodel any cyberworld object: the phone one uses in the game, the car one drives, the medication one takes, the clothes characters wear, etc.

Though immersive 3D applications are obvious examples of flexible worlds, more prosaic examples abound. Common cyberspace individualization, from the consumer's point of view, appears as an individualized, private, personal relationship with the organization using the collected information.

Dynamic web-page structure allows a near-infinite variety in form and content, based on information collected from multiple sources. Examples include the following:

- Personalized advertisements in boxes and banners and inserts inside personal documents such as email (Hotmail, Acrobat Reader, Google toolbars, etc.) are placed by 'free' software packages. Portals offering 'free' email, such as Yahoo and Google, also put advertisements on their user interface, based on a content anaylsis of received and sent mail. The consumer accepts that the presence of such advertising is innocuous, since it does not represent a 'cost'. In some cases the advertisements divert allocated bandwidth or slow computer performance, but their cost is still seen as zero since no money is demanded.
- Advertisements disguised as 'suggestions' included in many media players, which automatically update links to Internet radio stations, news, entertainment or newly released products from the music/film industry. Users are encouraged to click on 'now playing' buttons and to explore commercial content.
- Icons and links to their and other commercial websites, placed on the user's desktop, in addition to Windows' 'start' menu items and browser 'favorites' or 'bookmarks' by almost all software packages.
- 'Personalized' services (My Yahoo, etc.) based on information given or collected during users' activities on the website (as well as on 'partner' sites).
- Banner ads, pop-up windows, interstitials (e.g. Unicast's Superstitial; Unicast 2007), 'gatekeeper' ads and multiple attempts to redirect users during normal web browsing, some with a fake user interface.
- 'Adware' – software especially designed to serve its distributor's clients' adverts on users' desktops. These include Aureate/Radiate, AdBreak, AdReady, Alexa, Comet Cursor, Cydoor, Doubleclick, DSSAgent, EverAd, eZula, Expedioware, Flyswat, HomePageWare,

SEBar, OfferCompanion, Hotbar, OnFlow, TimeSink, Web3000, Webhancer, Transponder, Wnad, ZapSpot, SurfPlus, AdvertBar, NetPal, CashBar, WurldMediaBHO, MessageMates, EWA, Ezsearchbar, CommonName, GoHip, DownloadWare, NetworkEssentials, ImiServerIEPlugin, TopMoxie, Lop.Com, BDE Projector, UCmore, OpenMe, JaypeeSysBHo, FlashTrack, NetRadar, NetZany, NetSource, NowBox, TrustToolBar, WinAd, Kontiki, 7faSSt Search, and iWonCopilot.

First (and often still) thought of as nuisances, these various strategies of cyberspace customization are evolving into highly sophisticated, seamless and, more importantly, *useful* and *enjoyable* adjuncts to everyday computer use. Most computer users do not mind advertising – in fact, some of the most accessed content on YouTube consists of uploaded television commercials. Most people do not hesitate to give out personal information if privileges or other rewards are offered, or even if they are not (in the case of surveys, for instance).

Flexible space, in turn, enables behaviour modification and further data collection. The choices made by the user constantly refine the available information and allow continuous behavioural analysis. This also creates a world where users are consumers, where an ever-increasing proportion of possible behaviours are commercial relationships. Through the information exchange and flexible space, formerly neutral and/or unpredictable activities (click-throughs, adjusting page preferences, choosing news content and the like) can be transformed into revenue-generating behaviours. Status, identity and habits can become inter-corporation sellable *products;* as with mass media, the final product is not content but *audience* (or readership). Personal information is at the centre of this structure and therefore acquires a corresponding commercial value.

Secure space

One extremely important aspect of consumer-constructed flexible space is personal, familial and general security. Four levels of protection behaviours can be identified. At the basic level, individuals may feel various degrees of personal responsibility for their own security in cyberspace, such as using adequate passwords, not leaving passwords on a sticky note on one's monitor frame or in a non-encrypted text file (with the name, 'mypasswords.doc'), being aware of the identity of those asking for personal information, having working and up-to-date anti-virus, anti-spyware and firewall applications, securing personal, wireless local-area networks, etc.

At the second level, individuals may also recognize a collective responsibility as members of a variety of social groups: one's family, one's workgroup on a LAN or contacts on a mailing list, for example. This responsibility involves watching not only one's personal behaviour but also that of others. Family members may also need protection from web content or from ill-intentioned individuals. Many forms of techno-fixes exist to replace actual physical presence, such as filters blocking offensive or pornographic content (the extent to which such filters actually work is a separate matter). Protection of a workgroup's integrity may involve the control of members' activities on the intranet and/or internet. Logging software may be required, possibly accompanied by the automated analysis of logging practices (time of day, duration, frequency, etc.).

At the third level, most of us are part of a number of private networks where varying degrees of administrative, corporate or professional surveillance and control are applied (in most cases, work environments). We are asked at the same time to use provided IT resources within set limits and to report those who do not.

Finally, we are also part of a traditionally public security environment, where official, state institutions are deployed. We are officially forbidden from taking part in a (growing) number of activities online and, consequently (perhaps in return), we expect to be protected against crime. As the state is bound by traditional borders, its relevance in cyberspace is questionable. However, a number of sovereignty-affirming strategies have started to appear. Those dealing with heinous crimes are particularly well received by the public, who in general view state action as the only proper response to such deviance. New laws imposing data retention on ISPs and heightened interception capacity by intelligence agencies (the National Security Agency NSA) has collected 2 *trillion* phone-connection records since 2002) are part of the new strategies. In Canada, the multiplication of interceptions by the Communications Security Establishment (CSE), NSA's counterpart, has raised extremely few eyebrows (CSE Commissioner 2006 2007).

Individuals are warned of the risks of identity theft, of the misuse of valuable information, of the illegitimate use of their computer and of defamation. Very little can be done to prevent the last eventuality. The first three, however, have become the centre of a flourishing personal cybersecurity industry. Many manufacturers now offer plug-and-play USB biometric readers intended to replace all passwords. The average laptop has a built-in fingerprint reader. Anti-virus, firewall, and anti-spyware packages are also for sale or are pre-installed on

new computers (some in the form of 'trial versions'). Most require a lifetime of subscriptions to the necessary updates. This security world functions much in the way traditional, meat-space private security does: it must first sell risk as a series of threats in order to sell risk management solutions. The presence of hackers, criminals, organized crime, foreign criminal organizations and other enemies is continuously used to convince 'law abiding' netizens to adopt more secure behaviours (for one example, see Symantec's 'Cybercrime stories' and 'Sandra's story' at Symantec 2007).

Of course, individuals are not only potential cyber victims but also cyber criminals. Anyone can violate copyright online by using copied software, images, information, music, video, etc., outside explicitly permitted limits. A growing number of these actions are officially labelled as crimes by western countries (Leman-Langlois 2005, 2006). Netizens are encouraged to police their own behaviour; they are targeted by 'education' campaigns devised by legal rights owners and their representatives – the Recording Industry Association of America (RIAA) in the USA, the Canadian Recording Industry Association (CRIA) in Canada, the British Phonograph Industry (BPI) in the UK and the Australian Recording Industry Association (ARIA) in Australia (e.g. BPI 2007; CRIA 2007). The ARIA (http://www.aria.com.au/) has a website devoted to 'Music industry piracy investigations': 'MIPI conducts investigative, preventative and educational activities in relation to music piracy in Australia' (http://www.mip.com.au). Visitors are encouraged to take the 'Am I a pirate?' test, in order to make sure they are using music files appropriately – simply having paid for them being no guarantee (MIPI 2007). The CRIA warns that p2p users are not only victimizing music industry professionals but also putting themselves at risk of multiple forms of victimization: Trojan horses, malicious code, pornography distributed to their children and many other frightening possibilities (CRIA 2007).

If education fails, civil suits and criminal prosecution may ensue (as of August 2007, the RIAA had sued 18,000 individuals; see FoxNews 2007). Criminal prosecution is also increasingly likely, with stricter laws and demands for more proactive law enforcement practices (in the first half of 2007, the USA had criminalized 'attempts' at copyright infringements and Canada had done the same for the mere in-theatre recording of motion pictures).

The cyberspace behaviour of individuals who are responsible for others is further controlled through other forms of risk. For employees, there is the risk of data theft by hackers or spies; for parents, there are risks that their children could be exposed to child

pornography or fall prey to Internet luring. Canada has a site devoted to cyberthreats against children at Cyberwise.ca. Cyberwise offers advice to parents, professionals, teachers, etc., as well as guides to increasing safety through 'true stories' of cyberhorror (one document is titled, 'Thousands of paedophiles on the net'; Cyberwise 2007). This is standard risk/neoliberal 'conduct of conduct' (Rose 2000: 325–7), where behaviour is controlled not through the threat of punishment but with mere 'information' about risks (O'Malley illustrates this point with control strategies aimed at drug users; 2004: 331).

Interestingly, Cyberwise is operated by Industry Canada through its Strategis portal 'Canada's business and consumer site'; see http://strategis.ic.gc.ca/, a remarkably apt illustration of the main points of this chapter – that control of behaviour in cyberspace is largely structured by the necessities of commerce.

Conclusion: information, surveillance and crime

We find ourselves at the juncture of a number of fascinating trends, some cultural, some geopolitical, some technological that, taken together, create a contingent context where privacy and personal information are being fundamentally redefined. It has become too late to argue for (or against) privacy in terms of secrecy of information, private life, anonymity – or in terms of the surveillants and the surveilled. These concepts assume that holders of information are reticent to share it, that surveillance is not consensual, that the targets, agents and beneficiaries of surveillance are always the same. More importantly, it will become progressively less useful to think of privacy as an intrinsic facet of one's inner sanctum. Projected outwards, personal information can be reflected back to the individual – as well as to others – as a customized, personalized world where life seems better. For now, this applies best to more exotic forms of virtuality, but current developments point towards the increasing integration of the cyber and the physical.

In this context, it is likely that forms of deviance involving the unauthorized use of personal information, if they do not interfere with commercial exchanges (as does the subversion of payment schemes), will gradually lose what little importance they have. Though valuable when part of an aggregate, the personal information of any individual is nearly worthless on its own. On the contrary, deviance from the rules set for the consumption of commercial content (such as copy and distribution rules) is bound to become a priority for criminalization.

As for the way we will treat the deviants, one aspect of the matter is fundamental. Beck's nuclear plants represented a risk because of the colossal power they harnessed. Cyberspace risks, on the contrary, are always presented as the work of ill-intentioned individuals or small organized groups. Cyberspace itself is never a threat; it is a neutral, cold, technological environment where boundless human desires can be satisfied. In short, cyberspace risks are not technological, they are criminal. Consequently, those most likely to be criminalized are individuals who misuse commercial information content. At the opposite end, those having the least to fear from the state's ability to criminalize are the corporate content producers and distributors – those who 'make' the commercial cyberspace.

So the state may be displaced from the centre, but it is never far. Furthermore, whether it is held by state agents or by others, most of the behaviour control power still radiates from the few towards the many. Though flexible space provides benefits to netizens, any transformation of reality within their power is strictly local, individual.

Under this new incarnation of 'privacy', can the old metaphor of the panopticon still be of use? Bentham's well-known design for the ideal prison was to be built as a circle of cells opening on a central surveillance tower. To provide an idea of constant surveillance despite the sensory limits of human wardens, the windows of the tower were to be darkened by curtains, hiding the occupants. Clearly, the central tower of surveillance, from which hidden guards watch a captive and atomized population, is no longer an entirely adequate representation of today's world of ubiquitous surveillance technology. Other aspects of the model, however, seem more durable.

First, the rediscovered problem of data concentration (now reborn in new laws being enacted by many countries that require data retention by communication service providers or that grant the police access to various private databases) shows that the state has not entirely given up its power to access and use information about citizens. It may, instead, simply be retiring from the business of database production and management. (In one interesting development, the US Federal Bureau of Investigation has offered to compensate ISPs for data retention costs; Washington Post 2007.)

Secondly, if panopticism can no longer be used to describe the structure of surveillance of entire societies, it remains a powerful model for local activity and analysis. For instance, in previous work (Leman-Langlois 2003) I have used a variation of the panopticon trope to account for the limited adoption of CCTV by police organizations

in Canada. One common misunderstanding of the panopticon image stems from a confusion of the concept with reality, or the rationale with the results. When Foucault argued that society is *disciplinary*, he meant that modes of behaviour control have changed, not that individual subjects are actually more 'disciplined' – more respectful of rules, less adventurous, etc. Panopticism, in the same way, does not entail *actual* total surveillance and behavioural control through constant visibility. It simply means that controlling deviance is *understood as a problem of visibility* (including the 'visibility' of data traces). It is not surprising, therefore, that another idea of Bentham's was to involve every citizen in the surveillance of all behaviours, multiplying the eyes of the authorities (quite like the 'Bullywatch London' project; bullywatchlondon.org).

Thirdly, behaviour modification is still the ultimate goal of surveillance. The flexible space created as a reflection of personal information aims at creating proper, 'docile' cyberconsumers. The docile cyberconsumer refrains from deviant behaviours, helps the authorities find deviants, maximizes expenses online, responds positively to the customized advertising they experience, constantly gives more information about themselves in order to get more products, more advertising and so on.

Fourthly, one of the main arguments of this chapter has been that surveillance is becoming radically diffused. It is now accomplished by infinitely varied actors, for infinitely varied purposes; it is directed at infinitely varied targets, for infinitely diverse beneficiaries. While the state has been the traditional focus of attention, surveillance is now more continuous, dispersed through multiple spheres of life (home, work, leisure, but also simply walking one's dog). In physical reality, one's activities may be recorded by the state, of course, but also by one's condo association, one's neighbour, one's employer, entities located around the world, one's clients, one's service providers, etc. In cyberspace, the capabilities for surveillance and for the communication, analysis and use of knowledge are limitless. The panopticon's potential (realized or not) to see everything is still an important aspect of all forms of technosurveillance.

Of course, with the distribution of surveillance come two other phenomena: counter-surveillance and resistance. As Brin (Chapter 2, this volume) points out, surveilling those who surveil us may produce a checks-and-balances effect. However, one must take into account that organized surveillance is more constant, more structured and more powerful than what individuals can ever hope to achieve, even if they dedicated their entire working time to the task (Marx

2006), and even if their target was as easy to watch as they are. It seems illusory to expect individual, or even collective powers of surveillance – if they could in fact be harnessed, organized and targeted – to equate to that of specialized entities. Furthermore, the current reality is that individual surveillance is more concerned with individual targets: people love to spy on other people, for fun (YouTube), for security (NetNanny, webcams aimed at child or elderly care givers) and for profit (information sold to media organizations). Finally, counter-surveillance assumes that individuals actually feel a need for counter-surveillance; in reality, as we have seen above, the collection, analysis and use of personal information are becoming a voluntary, appreciated and beneficial activity in which they are happy to co-operate.

Resistance to surveillance is more interesting. Dupont (forthcoming) lists two main forms of resistance: information encryption and voluntary anonymity. Though relatively easy to acquire and to use, the tools necessary to resist surveillance in this way are, in fact, almost unheard of by the vast majority of netizens – in short, they do not 'exist,' and the mere potential to resist is not, in itself, resistance. A great number of individual surfers do use fake names when registering on websites or give non-existing email addresses to defeat some of the annoyances of the web, particularly the tendency of many organizations to 'spam' their email lists. However, as we have already seen, this strategy is nonsensical in a growing number of areas where defeating the system voids any possible benefit that participation might have produced. In other cases, resistance or refusal to comply with data collection implies a series of real and/or perceived costs to the individual: penal cost for non-compliance with legal rules, risk increases for disregarding security protocols, financial costs for non-compliance with marketing schemes (loss of benefits, loss of access to lower prices, etc.), convenience and productivity costs for non-compliance with identification systems (for example, when turning off 'cookies' in one's browser).

This new world of privacy will have interesting implications for those who study technocrime. New possibilities for behaviour, criminalization, enforcement, private justice, market regulation, consumer discipline and many others, all occurring in an equally new, and constantly renewed, environment. The impact on theories based on opportunities, social capital, social learning etc., will have to be analysed. I suspect that the theoretical bases for criminology will need fundamental revision.

References

Alford, J. (2002) 'Defining the client in the public sector: a social-exchange perspective', *Public Administration Review*, 62: 337–46.

Ars Technica (2007) 'Attempted infringement appears in new House Intellectual Property Bill (http://arstechnica.com/news.ars/post/20070730-attempted-infringmen-tappearsin-new-house-intellectual-property-bill.html).

Baudrillard, J.(1970) *La Société de consommation: ses mythes, ses structures*. Paris: Denoël.

Beck, U. (1992) *Risk Society: Towards a New Modernity*. London: Sage.

British Phonographic Industry (BPI) *Illegal Filesharing Fact Sheet* (http://www.bpi.co.uk/pdf/Illegal_Filesharing_Factsheet.pdf).

Brodeur, J.-P. and Stéphane Leman-Langlois, S. (2006) 'Surveillance-fiction: high and low policing revisited', in K. Haggerty and R. Ericson (eds), *The New Politics of Surveillance and Visibility*. Toronto: University of Toronto Press.

Canadian Recording Industry Association (CRIA) (2007) *Facts about File Sharing* (http://www.cria.ca/filesharing.php).

Communications Security Establishment Commissioner (2006) *Annual Report 2005–2006* (http://csec-ccst.gc.ca/ann-rpt/2005-2006/index_e.php).

Communications Security Establishment Commissioner (2007) *Annual Report 2006–2007* (http://csec-ccst.gc.ca/ann-rpt/2006-2007/index_e.php).

Cyberwise (2007) *Des internautes pédophiles par milliers* (http://strategis.ic.gc.ca/epic/site/cybp-cybpa.nsf/vwapj/Article%2021%20-%20Des%20internautes%20pédophiles%20par%20millier.pdf/$FILE/Article%2021%20-%20Des%20internautes%20pédophiles%20par%20millier.pdf).

Dupont, B. (forthcoming) 'Hacking the panopticon: distributed online surveillance and resistance,' in M. Deflem (ed.), *Sociology of Crime, Law and Deviance. Vol. 10. Surveillance and Governance*. Oxford: Elsevier.

Etzioni, E. (1999) *The Limits of Privacy*. New York, NY: Basic Books.

Feeley, M. and Simon, J. (1992) 'The new penology: notes on the emerging strategy of corrections and its implications', *Criminology*, 30: 449–74.

Fischer, H. (2006) *Digital Shock*. Montreal: McGill-Queen's University Press.

Foucault, M. (1975) *Surveiller et punir, naissance de la prison*. Paris: Gallimard.

FoxNews (2007) 'Record industry demands $3,000 from 50 Ohio university students', (http://www.foxnews.com/story/0,2933,258041,00.html).

Garland, D. (2001) *The Culture of Control*. Chicago, IL: University of Chicago Press.

Garnham, N. (2000) ' "Information society" as theory or ideology: a critical perspective in technology, education and employment in the information age', *Information, Communication and Society*, 3: 139–52.

Haggerty, K. (2006) 'Tear down the walls: on demolishing the panopticon', in D. Lyon (ed.), *Theorizing Surveillance: The Panopticon and Beyond*. Cullompton: Willan Publishing.

Leman-Langlois, S. (2003) 'The myopic panopticon: the social consequences of policing through the lens', *Policing and Society* 13: 43–58 (reprinted in Kappeler, V. (ed.) (2006) *The Police and Society: Touchstone Readings* (3rd edn). Long Grove, IL: Waveland Press.

Leman-Langlois, S. (2005) 'Theft in the information age : music, technology, crime and claims-making', *Knowledge, Technology and Policy* 17: 140–63.

Leman-Langlois, S. (2006), 'Le crime comme moyen de contrôle du cyberespace commercial', *Criminologie*, 39: 63–81.

Leman-Langlois, S. and J.-P. Brodeur (2005), 'Les technologies de l'identification,' *Revue internationale de criminologie et de police technique et scientifique*, 58: 69–82.

Lessig, L. (2002) 'Privacy as property', *Social Research*, 69: 247–69.

Los, M. (2006) 'Looking into the future: surveillance, globalization and the totalitarian potential', in D. Lyon (ed.) *Theorizing Surveillance: The Panopticon and Beyond*. Cullompton: Willan Publishing.

Loyalty Group (2007) 'Full privacy comment' (https://www.airmiles.ca/arrow/login/FullPrivacyCommitment).

Lyon, D. (2006) 'The search for surveillance theories,' in D. Lyon (ed.) *Theorizing Surveillance: The Panopticon and Beyond*. Cullompton: Willan Publishing.

Mathiesen, T. (1997) ' The viewer society : Michel Foucault's 'panopticon' revisited', *Theoretical Criminology* 1: 215–34.

Mattelart, A. (2001) *Histoire de la société de l'information*. Paris: La Découverte.

Marx, G. (2006) 'Mots et mondes de surveillance, contrôle et contre-contrôle à l'ère informatique', *Criminologie*, 39: 43–62.

Music Industry Piracy Investigations (MIPI) (2007) *Am I a Pirate? Some Common Questions and Answers* (http://www.mipi.com.au/amiapirate.htm).

O'Malley, P. (ed.) (1998) *Crime and the Risk Society*. Aldershot: Ashgate.

O'Malley, P. (2004) 'The uncertain promise of risk', *Australian and New Zealand Journal of Criminology*, 37: 323–43.

Pew Internet (2000) *Trust and Privacy Online: Why Americans Want to Rewrite the Rules* (http://www.pewinternet.org/PPF/r/19/report_display.asp).

Pew Internet (2007) *Social Networking Websites and Teens: An Overview* (http://www.pewinternet.org/PPF/r/198/report_display.asp).

Register (2007) 'MySpace erases 29,000 sex offenders', (http://www.theregister.co.uk/2007/07/25/myspace_erases_offenders/).

Rose, N. (2000) 'Government and control', *British Journal of Criminology*, 40: 321–39.

Second Life (2007) 'Police blotter' (http://secure-web11.secondlife.com/community/blotter.php).

SecuritySpace (2007) *Internet Cookie Report* (http://www.securityspace.com/s_survey/data/man.200707/cookieReport.html).

Symantec (2007) *Cybercrime Stories*, (http://www.symantec.com/avcenter/cybercrime/index_page4.html).

Unicast (2007) *Unicast Online Ad Display Systems* (http://www.unicast.com/how-we-do-it/unicast-ad-display-systems.shtml).

Washington Post (2007) '*FBI seeks to pay telecoms for data*,' (http://www.washingtonpost.com/wp-dyn/content/article/2007/07/24/AR2007072402479_pf.html).

Whitaker, R. (1999) *The End of Privacy: How Total Surveillance is Becoming a Reality*. New York, NY: New Press.

Wood, J. (2004) 'Cultural change in the governance of security', *Policing and Society* 14: 31–48.