Privacy, Identity and Anonymity

Ian Kerr and jennifer barrigar

A comprehensive understanding of *surveillance* requires an appreciation of its relationship to other core social constructs such as *privacy, identity* and *anonymity.*

The relationship between these concepts is uneasy and sometimes divisive among scholars of Surveillance Studies. Perhaps one reason for this is that surveillance and privacy are often misunderstood as binary opposites. The relationship is, in fact, more nuanced. As sociologist Stephen Nock observed in his study of the implications of an increasingly anonymous society of strangers, '*A society of strangers is one of immense personal privacy. Surveillance is the cost of that privacy*' (Nock 1993: 1). To the uninitiated, Nock's quote seems counterintuitive—after all, how can surveillance and privacy be anything but opposites? Does not more of one imply less of the other?

What appears at first blush to be a zero sum game is in fact a set of interdependent relationships. For example, according to Nock, individuals actively participate in communities and are constantly monitored and assessed by other community members. From this assessment is derived a cumulative reputation about the individual, which in turn becomes its own key to future participation within that society. This leads to further communal assessment, a more in-depth reputational appraisal, future access and so on. Historically, these performances and assessments took place in the context of family and local community, where everyone (supposedly) knew everyone else. However, in a more geographically dispersed society, we are

This chapter is adapted from *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, Oxford University Press, 2009.

confronted with the absence of such easy community information sharing. Consequently, we have moved to the development of various proxies such as ordeals and credentials.

An ordeal is a form of integrity test—for example, a lie-detector or drug-test. In contrast, a credential is a token of trust such as a signature, a personal identification number or other 'official' verifications in the forms of educational degrees or driver's licenses (Nock 1993: 11-16). Such proxies function as a crude form of authentication of the individual, but do not provide the extensive, detailed performance review that community knowledge can provide. Indeed, though such proxies can confirm the identity or (presumptive) truthfulness of an individual, they usually leave open the question of how to make an assessment of trustworthiness of the individual who has been identified.

Considered from another perspective, the relationship between information management and identity remains an integral one. Constructing an identity through the use of symbolic representations is a matter of information control. Successfully negotiating what information is attached to us, who knows what information, and how that information is protected from others becomes increasingly difficult in a technological environment where people can steal, distort, or delete your identity.

No matter what perspective is adopted, it seems that our ability to manage our privacy, including the power to identify oneself or not, to speak or act anonymously or without reference to one's 'real' credentials, is not merely interrelated but perhaps even inextricably linked to the concept of surveillance. Just as our desire for functional privacy brings with it the necessity for surveillance, so too do the ever-growing collections of personal information and history and their corresponding public availability make necessary the ability to separate some of our performances from that person of record.

The network society

The further migration of society to the realm of 'cyberspace' (as today's technologically mediated relationships are colloquially understood) has exacerbated our reliance on credentials and other tokens of identification. The advent of the world wide web in the 1990s initially enabled everyone with access to a computer and modem to become unknown and in some cases invisible in public spaces—to communicate, emote, act and interact with *relative* anonymity. Indeed, since the impact of what one could say or do online was no longer limited by physical proximity or corporeality, it not only increased anonymity but also increased the range of connection/communication possible. The end-to-end architecture of the web's Transmission Control Protocol, for example, facilitated unidentified, one-to-many interactions at a distance. As the now famous cartoon framed the popular culture of the early 1990s, 'On the internet, nobody knows you're a dog.' Although this cartoon resonated deeply on various levels, at the level of architecture it reflected the simple fact that the internet's original protocols did not require people to identify themselves, enabling them to play with their identities, to represent themselves however they wished.

Network technologies fostered new social interactions of various sorts and provided unprecedented opportunities for individuals to share their thoughts and ideas *en masse*. Among other things, the internet permitted robust political speech in hostile environments. It allowed users to say and do things that they might never have dared to say or do in places where their identity was more rigidly constrained by the relationships of power that bracketed their experience of freedom. Anonymous browsers and messaging applications promoted frank discussion by employees in oppressive workplaces and created similar opportunities for others stifled by various forms of social stigma. Likewise, new cryptographic techniques promised to preserve personal privacy by empowering individuals to make careful and informed decisions about how, when and with whom they would share their thoughts or their personal information.

At the same time, many of these new information technologies created opportunities to disrupt and resist the legal framework that protects persons and property. Rather than embracing the freeing aspects of this technological change in mainstream ways, some instead began to exploit the network to defraud, defame and harass, to destroy property, to distribute harmful or illegal content, and to undermine national security.

In parallel with both of these developments, there has been a proliferation of various security measures in the public and private sectors designed to undermine the 'ID-free' protocols of the original network. New methods of authentication, verification and surveillance have increasingly allowed persons and things to be digitally or biometrically identified, tagged, tracked and monitored in real-time and in formats that can be captured, archived and retrieved indefinitely. More recently, given the increasing popularity of social network sites and the pervasiveness of interactive media used to cultivate user-generated content, the ability of governments, not to mention the proliferating international data-brokerage industries that feed them, to collect, use and disclose personal information about everyone on the network is increasing logarithmically. This phenomenon is further exacerbated by corporate and government imperatives to create and maintain large scale information infrastructures to generate profit and increase efficiencies.

In this new world of ubiquitous handheld recording devices, personal webcams, interconnected surveillance cameras, RFID tags, smart cards, global satellite positioning systems, HTTP cookies, digital rights management systems, biometric scanners and DNA sequencers, the space for private, unidentified, or unauthenticated activity is rapidly shrinking. Many worry that the regulatory responses to real and perceived threats have already profoundly challenged our fundamental commitments to privacy, autonomy, equality, security of the person, free speech, free movement and free association. Add in the shifting emphasis in recent years towards public safety and national security, and network technologies appear to be evolving in a manner that is transforming the structures of our communications systems from architectures of freedom to architectures of control. We are shifting away from the original design of the network, from spaces where anonymity and privacy were once the default position to spaces where nearly every human transaction is subject to tracking, monitoring and the possibility of authentication and identification.

The effects of shifting social and technological architectures

These apparent shifts in our social and technological architectures raise a host of issues that occupy but also transcend the legal domain. The ability or inability to maintain privacy, construct our own identities, control the use of our identifiers, decide for ourselves what is known about us and, in some cases, disconnect our actions from our identifiers will ultimately have profound implications for individual and group behaviour. It will affect the extent to which people, corporations and governments will choose to engage in global electronic commerce, social media and other important features of the network society. It will affect how we think of ourselves, the way that we choose to express ourselves, how we make moral decisions, and our willingness and ability to fully participate in political processes.

There is a fundamental tension mitigating our understanding of privacy, identity and anonymity. While privacy is usually understood as a fundamental human right, anonymity as a basic foundation of political free speech, and identity as something that must be self-directed and chosen, there is an increasing currency in the belief that information must be monitored, collected and stored with permanence, and assessed continuously in order to prevent significant social threats. These debates, and the perceived conflict between privacy and security, have become increasingly fraught since 9/11 and the attendant emergence of a security state, including a return to the 'crypto-wars' of the 1970s/1980s in the recent government proposals requiring that telecommunications providers redesign their infrastructure in order to facilitate identifiability of users where required by the state.

Increases in the ability to identify users, as well as technological evolutions that allow for ever-greater storage and analysis of personal information are also creating concerns around the public/private divide. This is happening in many different ways. States are seeking to regulate spam; keep records to allow identification of those who interact anonymously with users, especially youth; publicize data security breaches; and regulate directed/targeted advertising. Outside of state concern about private industries' collection, use, disclosure and retention/security of personal information, there is also a question of state access to that very information. Data protection legislation was originally directed at state personal information practices and, accordingly, places stringent rules on what information may be collected and by what means, as well as regulating its use, disclosure, etc. With the increase in private sector data collections, states are able to deputize private organizations, either formally or informally and thus gain access to these private data banks, which at least arguably may avoid some of the more stringent controls placed upon state organizations by data protection legislation. Finally, even where private organizations are not providing the state with access to their databanks, data is increasingly being collected, mined and used for a variety of profit-based activities.

The network society's shifting social and technological architectures further complicate the relationship between privacy, identity and anonymity, and their ultimate connection to surveillance. Each of these three concepts is briefly considered in turn.

Privacy

Larry Ellison is the CEO of Oracle Corporation and the 14th richest person alive. In the aftermath of September 11, 2001, Ellison offered to donate to the U.S. government software that would enable a national identification database, boldly stating in 2004 that '[t]he privacy you're concerned about is largely an illusion. All you have to give up is your illusions, not any of your privacy.' Ellison was, in fact, merely reiterating a sentiment that had already been expressed some five years earlier by his counterpart at Sun Microsystems, Scott McNealy, who advised a group of journalists gathered to learn about Sun's data-sharing software, 'You have zero privacy anyway. Get over it.' More recently, we've seen Facebook founder Mark Zuckerberg opine that social norms have changed to favour public sharing of information instead of privacy. Indeed, many if not most contemporary discussions of privacy are about its erosion in the face of new and emerging technologies. One need only scan the media today to see this sentiment repeated in various ways, from the twitter hashtag #privacyisdead to op-eds and speeches from figures both public and private.

To judge whether privacy is dead (or dying) we must first understand it (see also chapters by Rule and Stoddart in this volume). Many academics have characterized privacy as a fundamental human right that goes to the core of preserving freedom and autonomy, and is essential to the workings of a healthy democracy. The judiciary has on many occasions shared this point of view. For example, Justice Gérard LaForest of the Supreme Court of Canada once opined that, 'grounded in man's physical and moral autonomy, privacy is essential for the well-being of the individual. For this reason alone it is worthy of constitutional protection, but it also has profound significance for the public order. The restraints imposed on government to pry into the lives of the citizen go to the essence of a democratic state' (*R v. Dyment* 1988: 427).

While the character of privacy has, without question, become more diverse in light of technologies of both the privacy-diminishing and privacy-preserving variety, the existence of privacy rights will not simply depend on whether our current technological infrastructure has re-shaped our privacy expectations in the descriptive sense. There has been significant academic attention to the shifting 'reasonable expectation of privacy' standard used by courts and other decision-makers, and a general consensus remains that it is a normative rather than descriptive concept; *contra* Ellison and McNealy, it is not a like-it-or-lump-it proposition. However, recent work in the field relied upon by various courts, including the Supreme Court of Canada, suggests that our 'reasonable expectations' must be understood in the context of a broader theoretical understanding of the manner in which information emanates from private spaces to public places (Kerr and McGill 2007: 392-432). Theories such as this also support a growing consensus that the meaning, importance, impact, and implementation of privacy may need to evolve alongside the emergence of new technologies.

How privacy ought to be understood —and fostered —in a network society certainly requires an appreciation of and reaction to new and emerging network technologies and their role in society. At the same time, an appropriate regulatory approach must be cautious to avoid threat- or issue-specific responses that neglect to articulate or reinforce the larger social value of privacy. One well-known example is the U.S.'s *Video Protection Privacy Act of 1988* enacted after Justice Robert Bork's video rental records were released to the news media during his confirmation hearing to the U.S. Supreme Court. This is a perfect example of a law that is far too technology-specific. By narrowly focusing on a single technology, the Act had extremely limited application from the outset and is now, like the technology it sought to regulate, completely obsolete. This can be contrasted with a 'technology-neutral' approach, such as the one adopted in the OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.* The latter strategy involves the adoption of a set of 'fair information practice' principles — regulating collection limitation, data quality, purpose specification, use limitation, security safeguards, openness and individual participation— which have subsequently been applied to an extremely broad range of emerging information technologies (OECD Guidelines: 23 September 1980). By providing concrete and well-grounded guidelines for the collection, use and disclosure of personal information, this approach alleviates the need to re-write privacy law each time a new privacy-implicating technology comes along.

Given that the currency of the network society is information, it is not totally surprising that these fair information practice principles were re-characterized in Germany and, subsequently, by a number of other courts as the means of ensuring of 'informational self-determination.' Drawing on Alan Westin's classic definition of informational privacy as 'the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others' (Westin 1967: 7) many jurisdictions throughout Europe and around the globe have adopted the fair information principles mentioned above as the basis for data protection regimes. However, these principles and the laws that support them are not a panacea, as they have been developed and implemented on the basis of an unhappy compromise between those who view privacy as a fundamental human right and those who view it as an economic right. From one perspective, these laws are grounded in a human rights framework and aim to protect privacy, autonomy and dignity interests. From another, they are the lowest common denominator of fairness in the information trade. While some argue that data protection presumes the use and disclosure of personal information, creating (if anything) a limited right of control over what organizations do with one's personal information rather than 'true' privacy. There is little or no acknowledgement that one might wish to prevent anything being done with the information or, indeed, the information being collected at all.

Identity

While lofty judicial conceptions of privacy such as 'informational self-determination' set important normative standards, the traditional notion of a pure, disembodied and atomistic self, capable of making perfectly rational and isolated choices in order to assert complete control over personal information is not a particularly helpful fiction in a network society. Who we are in the world and how we are identified is, at best, a concession. Aspects of our identities are chosen, others assigned, and still others accidentally accrued. Sometimes they are concealed at our discretion, other times they are revealed against our will. Identity formation and disclosure are both complex social negotiations and, in the context of the network society, it is not usually the individual who holds the bargaining power.

Because the network society is to a large extent premised on mediated interaction, who we are—and who we say we are—are not self-authenticating propositions in the same way that they might be if we were close kin or even if we were merely standing in physical proximity of one another. Although we can be relatively certain that it is *not* a canine on the other end of an IM chat, the identity of the entity at the other end of a transaction may be entirely ambiguous. Is it a business partner, an imposter or an automated software bot? Indeed, it may be that we sometimes do not need to know (and in some cases might not care) whether our interlocutor has an authenticated identity. Other times – when dealing with finances or other extremely sensitive or personal information – it can be crucially important to ensure that access to this information is restricted to those with the proper authorization.

However, it is important to recognize that identification techniques can preserve or diminish privacy. Their basic function is to make at least some aspects of an unknown entity known by mapping it to a knowable attribute – essentially a new form of credentialing, intended to identify an entity as known or authorized. An identification technique is more likely to be privacy-preserving if it takes a minimalist approach with respect to those attributes that are to become known. For example, an automated highway toll system may need to authenticate certain attributes associated with a car or driver in order to appropriately debit an account for the cost of the toll. But to do so, it need not identify the car, the driver, the passengers or, for that matter, the ultimate destination of the vehicle. Instead, anonymous digital credentials could be assigned that would allow cryptographic tokens be exchanged through a network in order to prove statements about them and their relationships with the relevant organization(s) without any need to identify the drivers or passengers themselves. Electronic voting systems can do the same thing.

Other strategies have focussed not on collecting digital tokens from individuals themselves, but rather on the reputation an individual has achieved within her community. At its most basic, reputation is comprised of a record of interactions and past experiences. As Donath and boyd observe, '[m]ost of the qualities we are interested in about other people – is this person nice? Trustworthy? Can she do this job? Can he be relied on in an emergency? Would she be a good parent? – are not directly observable. Instead, we rely on signals, which are more or less reliably correlated with an underlying quality' (Donath and boyd 2004: 72). Reputation, while to some degree made up of signals, itself functions as a signal for such assessments. We assess these signals as we interact with others, and we refine and revisit our assessments with each interaction. As many scholars have noted, the role of reputation is inherently public – that is, while image is self-directed, reputation is by definition other-directed and derived. And it is derived for the purpose of functioning as a kind of social lubricant. As Nock has described, it facilitates relationships among strangers by reducing uncertainty and thus helping to create trust (Nock 1993: 124). Unsurprisingly, then, reputation has achieved ever greater importance and utility as the opportunity(s) for uncertainty have increased.

An examination of the interaction of self and other in the construction of identity and the necessary connection between privacy/identity and broader discussions about power, gender, difference and discrimination therefore requires a deeper understanding of not only the interrelationship of these concepts but also how federated identity and/or reputation may function as forms of surveillance that come not only to authenticate an individual but also to police mainstream norms of presentation and performance (barrigar 2007). Identity formation and identification can be enabled or disabled by various technologies—data-mining, automation, ID cards, ubiquitous computing and human-implantable RFID—but each of these technologies too has potential narrowing effects, reducing who we are to how we can be counted, kept track of, or marketed to.

Anonymity

Anonymity allows for the creation of a new identity for many people owing to the fact that they have yet to have any signs ascribed to them, be they positive or negative. Anonymity allows for a public display of oneself (real or fantasy) in that anonymity means that there is no way to verify these claims.

Recently, Google CEO Eric Schmidt has suggested that

> [p]rivacy is not the same thing as anonymity. It's very important that Google and everyone else respects people's privacy. People have a right to privacy; it's natural; it's normal. It's the right way to do things. But if you are trying to commit a terrible, evil crime, it's not obvious that you should be able to do so with complete anonymity. There are no systems in our society which allow you to do that. Judges insist on unmasking who the perpetrator was. So absolute anonymity could lead to some very difficult decisions for our governments and our society as a whole. (Kirkpatrick 2010)

Similarly, riffing on Andy Warhol's best known turn of phrase, an internationally (un)known British street artist living under the pseudonym 'Banksy' produced an installation with words on a retro-looking pink screen that say, '[i]n the future, everyone will have their 15 minutes of anonymity.' Was this a comment on the erosion of privacy in light of future technology? Or, was it a reflection of Banksy's own experience regarding the challenges of living life under a pseudonym in a network society? While Warhol's '15 minutes of fame' recognized the fleeting nature of celebrity and public attention, Banksy's '15 minutes of anonymity' recognizes the long-lasting nature of information ubiquity and data retention. Indeed, anonymity may be the only way to guarantee privacy in a world where information is stored about us and easily shared.

Although privacy and anonymity are related concepts, it is important to realize that they are not the same thing. There are those who think that anonymity is the key to privacy. The intuition is that a privacy breach cannot occur unless the information collected, used or disclosed about an individual is associated with that individual's identity. Many anonymizing technologies exploit this notion, allowing people to control their personal information by obfuscating their identities. Interestingly, the same basic thinking underlies most data protection regimes, which one way or another link privacy protection to an identifiable individual. According to this approach, it does not matter if we collect, use or disclose information, attributes or events about people so long as the information cannot be (easily) associated with them. Of course, the notion that anonymization of information is a permanent solution is really only workable if technology ceases to evolve and change — as it is, the uncrackable of today will be the freely-available of tomorrow. Similarly, a number of computer scientists have demonstrated various ways in which the ever-increasing amount of publicly available information allows anonymized information to be re-identified. Information that has been aggregated may also be put forward as 'safe,' but this too is uncertain and may depend on the amount of information made available, the size or specialization of particular pieces of information or locations, etc. Increasingly, the problem is that while actual identity information may have been stripped from the information, it becomes increasingly possible to re-identify that information because there are still parts of it that are identifiable in some way.

While anonymity enables privacy in some cases, it certainly does not guarantee it. As any recovering alcoholic knows all too well, even if *Alcoholics Anonymous* (A.A.) does not require you to show ID or use your real name, the meetings are anything but private. Anonymity in public is quite difficult to achieve. The fact that perceived anonymity in public became more easily achieved through the end-to-end architecture of the net is part of what has made the internet such a big deal. It created a renaissance in anonymity studies, not to mention new markets for the emerging field of identity management. The A.A. example illustrates another crucial point about anonymity. Although there is a relationship between anonymity and invisibility, they are not the same thing. As some leading academics have recently come to realize, visibility and exposure are also important elements in any discussion of privacy, identity and anonymity. Indeed, many argue that the power of the internet lies not in the ability to hide who we are, but in freeing some of us to expose ourselves and to make ourselves visible and/or heard on our own terms.

With the increase in avenues for comment and discussion via online spaces, we have seen a corresponding increase in legal actions where identification and identifiability are at the crux of the matter. Especially in areas such as cyber-bullying, cyber-harassment and cyber-stalking there is much speculation about how anonymity may enhance the abuser's power or even encourage behaviour that would not necessarily be performed were it visibly attached to an offline identity. Where currently U.S. and Canadian courts facilitate identifiability upon commencement of suit, questions arise as to whether filing a full legal suit is necessary or appropriate where it is only this identification that is desired. Recognizing that identifiability often translates into accountability, James Grimmelman has posited (though he subsequently rejects) a system where complainants could trade their right to future legal remedies for reputation harm in exchange for learning the name of the person (or persons) responsible for a particular harmful posting or comment. Alternatively, Daniel Solove has proposed that people be able to sue without having their real names appear in the court record, thus allowing people to seek a remedy for the spread of information about them without having to increase the exposure of the information.

Given its potential ability to enhance privacy, on the one hand, and reduce accountability on the other, what is the proper scope of anonymity in a network society? A recent study of anonymity and the law in five European and North American jurisdictions suggests that the law's regard for anonymity is to some extent diminishing (Kerr et al. 2009: 437-538). Despite significant differences in the five legal systems and their underlying values and attitudes regarding privacy and identity, there seems to be a substantial overlap in how these legal systems have historically regarded anonymity—not generally as a right and certainly not as a foundational right. What seems an indisputable global trend is that that anonymity is, once again, under fire. Interestingly, it appears that legal treatment of anonymity varies not from jurisdiction to jurisdiction as much as it does between subject matter. That is, in each jurisdiction reviewed, anonymity has been positioned as anything from a fundamental right to a fundamental non-right, depending on the subject matter of the complaint. Rather than explicitly recognized as a human or legal right, anonymity is instead found as an aspect of other concepts, and while it is highly valued and protected in the context of political speech, it does not receive the same treatment in other areas. To some degree, this accords with our own relationships with anonymity—although we speak of anonymity as integral to privacy and privacy a fundamental human right, we must also recognize the extent to which identity is performed (and ascribed in response to performance) and interrogate whether true anonymity (and its resulting indistinguishability) is itself desired or whether it too becomes a (linguistic) proxy for privacy.

When one considers these emerging legal trends alongside the shifting technological landscape, it appears that the answer to our question posed at the outset is clear: the architecture of the network society seems to be shifting from one in which anonymity was the default to one where nearly every human transaction is subject to monitoring and the possibility of identity authentication. The implications of this are far reaching, as the following case study suggests.

Case Study

Diary of a London Call Girl is a site that debuted in 2003 and purported to relate the experiences of a young woman as she began and continued to work for a London Escort Agency. The author identified herself by the pseudonym 'Belle de Jour.' As the site became more popular and the franchise grew to include published books and a spin-off television series, there was much public speculation as to Belle's 'real' identity. There are various explanations as to why this dual 'self' came to an end—Dr. Brooke Magnanti has suggested that an ex-boyfriend was on the verge of outing her, and an independent blogger has claimed to have noticed searches that suggested her identity was about to be reconciled and publicized. Accordingly, on November 15, 2009, Dr. Magnanti outed herself as Belle de Jour (Ungoed-Thomas 2009). Dr. Magnanti is a research scientist at Bristol University in the UK, and has stated that she was employed by an escort agency for 14 months while completing her Ph.D. thesis. (Ungoed-Thomas 2009).

The use of the pseudonym 'Belle de Jour' allowed Dr. Magnanti to anonymously journal her experiences and commodify the popularity of her site while continuing her education and advancing her academic career. Interestingly, since the revelation, although each had investments in particular aspects of her 'self,' both the university and her publisher have been publicly supportive of the decision, with Bristol University stating that Dr. Magnanti's past was irrelevant to her university position, and her publisher lauding her for the courage it had taken to come forward. The management of information and identity arguably enabled her to become established in both areas, such that the reconciliation was not destructive to either of her two identities.

An entry on her blog the day of the public revelation spoke about the importance of reconciling the different aspects of her personality, and denied that her offline self was any more 'real' than her pseudonymous online self. Both in her decision to identify herself and in her subsequent comments, Dr. Magnanti demonstrates many key aspects of the interrelationship between privacy, identity and anonymity. Choosing to control information about her via the use of a pseudonym allowed her the privacy and freedom to develop her selves without confusion or dissonance emerging between them. That is, the Belle de Jour (id)entity was able to expand her reach and brand without being accused of being fictitious or merely a product of Dr. Magnanti's imagination, since few in the mainstream would comfortably accept that sex work would be performed by a well-known academic researcher. At the same time, Dr. Magnanti was able to pursue a doctorate and then an academic career without worrying that Belle de Jour would compromise her opportunities or access to academic success. Dr. Magnanti spoke explicitly in her journal entry about the revelation and about the power of anonymity to allow voices that might otherwise be silenced to be heard—in this situation, anonymity allowed not only her voice to be heard in dual spheres, but also permitted her to protect her privacy and develop those identities concurrently.

Conclusion

Dr. Magnanti is not the first nor will she be the last to experience a loss of control over her personal information, pressure to identify herself and a diminishing ability to remain anonymous. As we migrate further and deeper into electronic environments, as our life chances and opportunities are further influenced by information intermediaries, social networks, ubiquitous computing, social sorting, actuarial justice and many other surveillant forces, it is suggested that the norms underlying privacy, identity and anonymity will continue to increase not only in their complexity but also in their broad social significance.

References

barrigar, J. (2007) 'i want you to want me: the effect of reputation systems in online dating sites,' *On the Identity Trail*, 13 February. Online. Available HTTP: <http://www.anonequity.org/weblog/archives/2007/02/> (accessed 13 November 2010).

Donath, J. and d. boyd. (2004) 'Public Displays of Connection,' *BT Technology Journal,* 22 (4): 71-82.

Kerr, I. and J. McGill. (2007) 'Emanations, Snoop Dogs and Reasonable Expectation of Privacy,' *Criminal Law Quarterly,* 53(2): 392-432.

Kerr I., V. Steeves and C. Lucock (eds) (2009) *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society,* New York: Oxford University Press.

Kirkpatrick, M. (2010) 'Google CEO Schmidt: "People Aren't Ready for the Technology Revolution,"' *ReadWriteWeb*, 4 August. Online. Available HTTP: <http://www.readwriteweb.com/archives/google_ceo_schmidt_people_arent_ready_for_the_tech.php> (accessed 7 November 2010).

Organization for Economic Co-Operation and Development. (1980) *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Online. Available HTTP: <http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html> (accessed 7 November 2010).

Nock, S. (1993) *The Costs of Privacy: Reputation and Surveillance in America,* New York: Aldine de Gruyter.

R v. Dyment [1988] 2 S.C.R. 417.

Ungoed-Thomas, J. (2009) 'Belle de Jour revealed as research scientist Dr Brooke Magnanti,' *The Sunday Times*, 15 November. Online. Available HTTP: <http://entertainment.timesonline.co.uk/tol/arts_and_entertainment/books/article6917260.ece> (accessed 13 November 2010).

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