

Intimacy 2.0: Privacy Rights and Privacy Responsibilities on the World Wide Web

Kieron O'Hara

School of Electronics and Computer Science
University of Southampton
Highfield
Southampton
United Kingdom S017 1BJ

kmo@ecs.soton.ac.uk

ABSTRACT

This paper examines the idea of privacy in the world of 'Intimacy 2.0', the use of Web 2.0 social networking technologies and multimedia for the routine posting of intimate details of users' lives. It will argue that, although privacy is often conceived as a right with benefits that accrue to the individual, it is better seen as a public good, whose benefits accrue to the community in general. In that case, the costs of allowing invasions of one's privacy do not solely fall on the individual who is unwise enough to do so, but also on wider society.

Keywords

Privacy, social networking, public and private goods, privacy rights, Web 2.0, Intimacy 2.0, communitarianism, liberalism

1. INTRODUCTION

The status of privacy is much disputed in political philosophy. An important debate has been conducted over the last couple of centuries as to whether it is a human right, or merely a preference. If there is a right to privacy ("the right to be let alone"), as was argued in a classic paper by Warren and Brandeis [33], then everyone, regardless of culture, ethnicity or nationality, is entitled to protection. If not, then it is merely a preference, however powerful, which there is no *obligation* to protect. Most major legal jurisdictions recognise some rights to privacy.

In all cases, the right to privacy is recognised as potentially in conflict with other rights, most obviously to free speech. Furthermore, many people enjoy a certain level of exhibitionism (also pandering to a certain level of voyeurism in their audience). Television programmes like the *Big Brother* franchise and confessional talkshows such as that hosted by Jerry Springer have not only big audiences, but also long waiting lists of potential participants.

Technology in particular can alter the boundaries between public and private. In 1890 Warren and Brandeis were concerned about the development of the portable camera, but in recent years the World Wide Web, particularly Web 2.0, has raised challenges for privacy, as it brings together more voices, more recording and retrieval technologies, and a larger capacity for the incidental gathering of details of people's private lives [15]. Interactive Web 2.0 technology has led to an increasing tendency for people to

publish texts, photographs, videos, locations, tags and preferences online, thereby placing a good deal of private life on record [21]. Facebook founder Mark Zuckerberg has argued that social changes mean that privacy is no longer a norm [11]. I call this tendency 'Intimacy 2.0'.

Whether privacy is a right, is essential, or is harmful to the community is a topic of ideological dispute, but the disputants agree on one thing: that privacy is basically a private good, whose benefits accrue to the individual [6], and which pits the interests of the individual against those of the community. In many circumstances there is a justifiable social benefit from breaches of privacy [8].

I shall dispute this common ground in the context of Intimacy 2.0. I will be concerned solely with the supposedly least problematic case: people releasing information that (a) is true, (b) directly concerns themselves, and (c) if it harms anyone at all, directly harms *only* themselves. I will argue that even in these cases, privacy is not only a private good, but also a public good, some of whose benefits accrue to the community. As such, our rights to privacy need to be balanced with responsibilities to preserve privacy.

2. PRIVACY AS A PRIVATE GOOD

In this section I will rehearse the thinking behind the idea that privacy is a private good, focusing on two opposed ideological views, liberalism and communitarianism.

2.1 The Liberal Argument

Liberalism is intended to protect the individual's freedom, not only to do what others reckon he or she *ought* to do, but what he or she *wishes* to do. Liberalism removes restrictions not only on action, but also on the definition of the good life. The classic text is John Stuart Mill's *On Liberty* [18], where what we can call the *Mill test* delineates the proper scope for community action. "That the only purpose for which power can rightfully be exercised over any member of a civilized community, against his will, is to prevent harm to others. His own good, either physical or moral, is not a sufficient warrant."

2.1.1 The Value of Privacy

People may prefer privacy, but that does not of itself obligate societies to protect it; after all, I have a strong liking for champagne but I have no claim on others to provide me with it, to my deep and abiding regret. Privacy must play some kind of

important role beyond being merely pleasant, in order for people to have a *right* to it.

Liberal theorists locate this role in the protection of *autonomy*, that is informed and uncoerced freedom. To act freely, a person should have accurate expectations of what is known about her; “only on the basis of the (fragile) stability of her fabric of expectations, knowledge, assumptions and selective self-disclosure is it possible for a person to exercise control over her self-presentation and thus, in a broader sense, to enjoy the possibility of a self-determined life” [26]. Note that this control needs to be authentic and not merely a (possibly mistaken) perception; if someone *falsely* believes that a certain piece of information has been kept private, and on that basis believes she is acting autonomously, she is nevertheless *not* doing so. Her behaviour, though uncoerced in the sense of meeting her preferences, is not informed, because her understanding of the situation is distorted, and her preferences have been formed in misleading circumstances.

Hence the point of privacy is to maximise the accuracy of the individual’s expectations of others’ views of her, and therefore to increase her ability to act autonomously. Privacy plays a central role in the liberal view of free action, and is hence much more than a mere preference.

2.1.2 Privacy as a Right

On the liberal account, therefore, privacy is an individual’s right that helps secure his or her autonomy in a complex and demanding world. If a person wishes to give his or her privacy away, by placing details on the Web, appearing on *Big Brother* or simply wandering around naked with the curtains open, it follows from this that they are harming themselves by reducing their ability to act autonomously. They do this presumably because they believe that they will get greater benefits without privacy than with it. We may believe that they are wrongheaded, but if we apply the Mill test we have no liberal ground for preventing them.

2.2 The Communitarian Argument

Liberal protection of individuals’ freedom has social costs. The ideology known as *communitarianism* maintains that individual freedoms only make sense against the background of a well-functioning community, and therefore when individual rights undermine community health they need to be curbed. Amitai Etzioni has argued that privacy rights have the potential to undermine community cohesion [8]. He claims that privacy is a contingent concept dependent on culture-specific assumptions and legal prohibitions. Far from being universal, it is being reformulated all the time (for example in Web 2.0); far from being an unbounded good, it should be balanced against other social concerns.

Communitarians are not opposed to privacy *tout court*, and represent themselves as being better protectors of privacy than liberals, whom they see as failing to provide a congenial context for a rewarding private life. For instance, most of our protection from social and political tyranny comes from our associations, which we support with feelings such as loyalty, conformism and shame, precisely the sort of surrender of privacy and autonomy that the liberal rejects [27].

2.3 Technical and Legal Discourse

Given the tacit agreement on this issue between otherwise radically opposed ideologues, it is not surprising that most legal and technical discourse adopts the same assumption. For instance, the privacy activism website Pleaseroame.com¹ publishes a live feed of Twitter posts which have revealed that their authors are not at home. The anticipated harm is that the author him- or herself may have given away too much personal information and created a personal vulnerability. Privacy-enhancing technologies are aimed at the individual, driven by fears of fraud, identity theft and loss of large databases, and are intended to give people control over their information when they use the Internet [10]. Companies such as Garlik² and Reputation Defender³ provide services to help data subjects control their individual digital footprints.

In US law, privacy is conceived as a tort, i.e. a harm to an individual for which another is responsible. There are two points to note. First, the individual who is the subject of the information is the direct and only victim of the tort, as the liberal and communitarian argue. Second, in the cases we are considering, the information about the victim is released by him- or herself, thereby being responsible for the harm, ruling out any possibility of a tort.

Another type of approach pursued in Europe is data protection, legal protection of individuals with regard to the processing of personal information [32]. This approach is even clearer in its assumption of where the benefits and costs of privacy will be found, as it explicitly balances the privacy of the individual with the benefit for society of information aggregation and processing [22].

3. INTIMACY 2.0

The conception of privacy of Section 2 is ultimately self-defeating if people see a benefit from rejecting it. They may have a right to it, but equally it is a private good, and so only they benefit from it. It seems to follow that only they suffer from their ignoring it. In this section I will examine how this behaviour plays out in Web 2.0.

3.1 Behaviour

Intimacy is an important aspect of healthy interpersonal relations, a key part of which is information-sharing and self-revelation. In the Web 2.0 world, Intimacy 2.0 is also achieved partly by self-disclosure [12]. Online disclosures are searchable, replicable and quasi-permanent, unlike the offline world where memory is the main medium. Furthermore, it is harder to track who has had online access to information, and to erect online obstacles to strangers or enemies getting hold of it. Nevertheless, people have a stronger tendency to self-disclosure online than offline [12].

Intimacy 2.0 reverses the standard (Weberian) view of trust where trustworthiness precedes and causes trust, and is governed by a (Durkheimian) view where trust comes first and trustworthiness later [20]. Many social networkers, bloggers and online diarists assume that readers will be sympathetic and worthy of the

¹ <http://pleaseroame.com/>.

² <http://www.garlik.com/>.

³ <http://www.reputationdefender.com/>.

intimacies revealed, and look forward to mutual revelation and intimacy, even though these assumptions are often incorrect [7]. This relative lack of filter is an important difference between intimacy in the offline world and Intimacy 2.0.

Surveys (e.g. [13]) have shown a relative lack of concern about privacy, while actual behaviour is even less protective than users believe or claim [12]. Users of social networking sites believe that they have more control over their information than they actually have, although as noted they also trust that (most of) those who have access to information about them will be benign. Some protect privacy by posting some inaccurate information. Some believe that privacy protection is in effect futile, and their continued networking implies they indeed have few privacy concerns. Equally, outcries over services perceived to have 'crossed the line' imply that there *is* a line that can be crossed. The outcries also show that social networkers are vigilant about issues that concern them. For instance, in November 2009 Facebook supposedly simplified its complex privacy policies, but many suspected that the aim was to get people to publish more information than before, thanks to new defaults and a few tweaks to valuable sources of information [3].

3.2 “Get Over It”: Technological Determinism

It is in this context that Zuckerberg made the remarks discussed at the beginning of this paper [11]. Privacy has always been under threat as soon as digitised information began to erode the practical obscurity that paper-based storage affords [21]. As early as 1999, Scott McNealy, then-CEO of Sun Microsystems, famously announced “you have zero privacy anyway. Get over it!” [16].

This technological determinism rests on the assumption that Web technology (and specifically social networking and Intimacy 2.0) can empower its users in such a way as to compensate them to their own satisfaction for any loss of autonomy (as we shall see in the next subsection, it may anyway provide mechanisms which preserve autonomy). As this only harms themselves (by the hypothesis of section 2 above), then the Mill test prevents others taking action to protect them against themselves. In any case, because the Web's basic design is an everything-goes knowledge sharing technology, building deep privacy protection into it would cripple its decentralised structure, which most would agree would be a far greater harm than the destruction of privacy. Finally, use of the Web is voluntary, and therefore there is no tort which can be seized upon – as the privacy-invading nature of the Web is well-understood, the user himself is largely responsible for any loss of privacy.

So: get over it!

3.3 The Generation Gap

Technological determinism also has a social aspect, because young people are substantially less concerned about privacy than the rest of us, and since they will be dead less quickly their attitudes will be more influential on future trends.

Work by Abril has indicated that one important generational shift is in the very concept of privacy under consideration [1]. Whereas older people see privacy as a matter of *control* – one has the luxury of determining how information about oneself is disseminated – young people see it as *anonymity* – they surrender control over dissemination on the assumption that information

cannot be traced back and associated directly and publicly with its subject, even if it is not private in the sense of being controlled by the subject. Anonymity may help support autonomy if control is absent, because even if the information about a person is in the public domain, if it cannot be associated with her then it does not materially affect her expectations of what is known about her.

This focus on anonymity chimes in with a point made by danah boyd that teenagers' offline privacy concerns are mostly to do with keeping information away from teachers and parents. They have very little control of context in the way that an adult has (e.g. the occupier of a house has rights to prevent unauthorised access, whereas parents cannot be kept out of a teenager's bedroom), and so are more concerned with controlling audiences by finding unmediated spaces in which to socialise [5]. However, that does not mean that they have a good grasp of how to do that [4], [5], [24], and indeed they do not have much of an idea of how much and what is being collected about them by third parties [24].

In particular, young people tend to consider how the people they know will access and respond to their profiles, and consequently put a lot of potentially sensitive information in them. 55% of US teenagers online have social network profiles, in which 82% include a real first name, 79% images of themselves and 49% the name of their school [14]. In practice, the anonymity that youngsters crave is harder to find than they often believe [7]. They place Durkheimian trust in their social networking friends, but they are often unaware that, via their social network sites, they are connected with a far larger network of corporations, institutions and individuals [24].

The law, on this issue, is a ‘digital immigrant’, supporting control rather than anonymity. However, the online world is not very geared towards control and hence the law lags behind. It provides the wrong sort of protection for those who crave anonymity, and inadequate protection for those who would prefer control [1].

Up till now I have left unexamined the argument of section 2 that privacy is a private good. In the next section, I will consider some reasons for thinking that the harms of a breach of privacy may be distributed more widely.

4. PRIVACY AS A PUBLIC GOOD

Most discussion of privacy has focused on harms to the individual, either the self-revealer or others who are directly implicated in information revealed. For instance, a recent ‘map’ of the territory focuses almost entirely on the individual [15], looking at actors and relationships that can take part “in a privacy incursion”. Of course this is part of the picture, but it ignores the cases where what is important is a *pattern* of privacy incursions, an *array* of actors and an *emergent* harm. Solove draws attention to the creation of a ‘culture of unease’ [30], but it is my contention that societal harm can go further than this, and in this section I will suggest some of the ways.

4.1 Pollution of Public Space: The “Tyranny of Intimacy 2.0”

Sociologist Richard Sennett has examined the imbalance between public and private experience, arguing that “intimacy is a tyranny” and that it is “a field of vision and an expectation of human relations ... a localizing of human experience, so that what is close to the immediate circumstances of life is paramount” [28]. Similarly, Hannah Arendt drew attention to the importance for the

quality of public life of putting distance between it and the private sphere. For her, “the reality of the public realm relies on the simultaneous presence of innumerable perspectives ... for which no common measurement or denominator can ever be devised” [2]. She follows Machiavelli in insisting that personal virtues such as ‘goodness’ (and indeed ‘badness’) have no place in public life, where more utilitarian and social qualities such as ‘effectiveness’ and ‘justice’ are needed.

Sennett warns of intimacy tyrannically denying “the reality and worth of impersonal life.” High quality public decision-making demands objectivity, evidence-based policy and authoritative behaviour, yet the spread of intimacy and the ease of transmission of intrusive detail has turned public life into a celebrity-driven circus where politicians are judged on the basis of whether we would want a beer with them, rather than their intellectual or managerial capabilities. Intimacy 2.0 has led to the ubiquity of politicians on Web 2.0 platforms. Political philosophy is now reduced in complexity to the level of a tweet, and the length of pause allowed for reflection is being shortened as political discourse moves in blogosphere time [25]. This can only make the private lives of politicians more public than they already are, undermining the impersonal life that Sennett wants to defend.

4.2 Web 2.0 and the Development of Identity

A profile provides a means of creating and controlling identities. Young people in particular, whose identities are malleable and who are interested in exploration and creativity, find this important [1], [5], [24]. Links with the identities of others (and other online resources) are important tools here [23], and hence an online presence seems key to the effective use of this identity-exploring mechanism. The potential for embarrassment and shame in Intimacy 2.0 is problematic in this context. As Martha Nussbaum has argued, shaming produces an enduring reduction in social status, and a degraded identity [19], hardly the empowering phenomenon that advocates of the technology might hope for.

Although an adult personality is not in such a state of flux, we negotiate different types of context with different methods of self-preservation, as Goffman argued many years ago [9]. Different personas are crafted for varying levels of public or private consumption, and the Web has quickly become an important space for experimentation with identity. “On the one hand, we maintain an attitude of external distance; ... this way you can relax, you are delivered of the burden of being what you are. ... On the other hand, the screen persona I create for myself can be ‘more myself’ than my ‘real-life’ persona ... in so far as it reveals aspects of myself I would never dare to admit in real life” [34]. Hence a chilling effect caused by bad experiences with Intimacy 2.0 will be as devastating to the identities of adults as those of younger people.

4.3 Emergent Associations

As well as identity, the associations we form are also important to provide an agreeable social context, and to act as protection against social pressures [27]. Relational data can be extremely important for extracting information about associations, and also about the individuals in the associations (even those who do not feature strongly in the data). Traffic data and clickthroughs can provide an accurate picture of technologically mediated emergent associations, and it has been argued that existing legal paradigms in the US have failed to protect such associations from snooping using network analysis [31].

Facebook can assemble a network of acquaintances of an individual Facebook user, allowing non-Facebook users to receive emails demonstrating Facebook’s knowledge of their own lives. An example: I received an email on 15th February 2010 suggesting nine Facebook people I may know – I knew seven of them, three of them quite casually (one of whom I had not contacted for five years). The harm to me was not high, but it is extraordinary that Facebook could so easily assemble such information about someone who has tried to avoid dealings with it (what could an authoritarian government do with this technology?), yet my privacy from Zuckerberg and his minions has been reduced *not* by my own actions, but by those of others.

4.4 Reasonable Expectations

One of the most important pillars of privacy protection in law is that of *reasonable expectations* [17]: one’s privacy is protected when one is in a context where a reasonable person should expect privacy, and not otherwise. This is a normative concept, and so is not completely undermined by Zuckerberg-style technological determinism. McArthur argues [17] that key factors in determining reasonable expectations are the *mischance principle* that we cannot reasonably expect something to be private that someone could easily discover without much effort (even if in fact it is discovered with difficulty), and the *voluntary principle* that our reasonable expectations are proportional to our efforts to protect our privacy. On this basis, he argues that Internet browsing histories and emails cannot be reasonably expected to be private.

This dodges the important question. The mischance principle allows a substantial mismatch between the effort needed to get the information and the effort actually expended. As an example, I can’t reasonably expect my purchase of *The Communist Manifesto* to be private, as I bought it in a bookshop and people could see it in my hand at the till, even if my complaint is about someone who found out through some more intrusive method. But this seems a very permissive principle in the case where someone has aggregated *all* the facts about me that someone *might* collect via a mischance in a database, and is performing inference across that database to discover patterns beyond the data. This kind of behaviour by information-based companies stretches the mischance principle a long way.

Furthermore, it ignores the distinction between private and public harm. If a significant minority (or majority) of people behave in such a way as to lower their own reasonable expectation of privacy, and if ‘reasonable expectation’ is a normative concept across a society, then they have lowered *my* reasonable expectations. My expectations could be very high, but the actions of others could turn them from reasonable to unreasonable (it is for this reason that Etzioni thinks reasonable expectations are a bad guide [8]).

Recall my intrusive email from Facebook. On McArthur’s argument, my reasonable expectations are neither here nor there because of the mischance principle; none of these relationships was a *secret*. Yet only a giant corporation with access to gross amounts of data and computing power could have assembled this information. As Solove argues, “a more nuanced view of privacy suggests that [Web 2.0 cases involve] taking an event that occurred in one context and *significantly* altering its nature – by making it permanent and widespread” (my emphasis) [29]. There is a massive transformation between storing and cataloguing. The

Web 2.0 context turns the mischance principle into the largest loophole imaginable.

Reasonable expectations are closely linked with social norms, yet it is arguable that online social norms are less embedded and more vulnerable to manipulation. Assumptions, knowledge and behaviour of Web users are highly heterogeneous (much more so than offline), and so the protection reasonable expectations provide may be naturally low anyway. Intimacy 2.0 undermines them further.

4.5 The Death of Autonomy

The net result of all this is a dramatic reduction in autonomy. As Abril argues, “the more people hear stories of others getting ‘busted’ on [social networks], the less likely they will be to share their stories and opinions. ... We can no longer erase or ignore our pasts. Such surveillance changes behaviour. Awareness of monitoring can make a person feel extremely uncomfortable and ultimately lead to self-censorship, inhibition, and a chilling of discourse” [1]. Although free speech is vital for democracy, so is privacy: “more discourse about politics occurs in personal conversations than on soapboxes or street corners” [29]. Intimacy 2.0 in effect blurs the distinction between personal conversation and soapbox (in the same way as social networking has blurred the distinction between friends and acquaintances).

Most benefits of autonomy accrue to the individual, but the ability of people to behave autonomously is also a mark of a good society (cf. Orwell’s *1984* as a description of society without autonomy). If Intimacy 2.0 reduces our collective capacity for autonomy, then that is an additional public harm.

5. CONCLUSION: PRIVACY RIGHTS AND PRIVACY RESPONSIBILITIES

The upshot of the arguments of the previous section is that the unwise behaviour ceases to be ‘only’ self-harm and becomes a type of environmental pollution, thereby *failing* to meet Mill’s test. For the liberal, the importance of Intimacy 2.0 must now be measured, not against self-harm, but harm to the community.

These arguments also apply to communitarians, even though they do not value privacy as highly, because of the indirect harms to the community. In the Intimacy 2.0 context, Etzioni’s claim that the community rights trump individual privacy rights *entails* that people should preserve their privacy. In short, as well as the privacy *rights* that are championed by the liberal, the communitarian must agree that there are privacy *responsibilities* too.

This normative claim requires enforcement mechanisms, which may take the form of regulations, technological measures or ideally social norms. However, consideration of the possibility of norms of behaviour developing that enable people to internalise these privacy responsibilities (which the McNealy/Zuckerberg technological determinist position claims is impossible) must be deferred to another paper; for preliminary discussions about technical and legal issues see [1], [15], [22] and [29]. Methods to measure self-disclosure in its context must also be developed [12]. Perhaps the most effective step will simply be raising awareness [21], as psychological research has shown that people primed to think about privacy issues will disclose less about themselves [12].

6. ACKNOWLEDGMENTS

The work reported in this chapter was partly supported by the projects LiveMemories – Active Digital Memories of Collective Life, Bando Grandi Progetti 2006, Provincia Autonoma di Trento, and the EU FET project Living Knowledge, (<http://livingknowledge-project.eu/>), contract no. 231126.

7. REFERENCES

- [1] Abril, P.S. A (My)Space of one’s own: on privacy and online social networks. *Northwestern Journal of Technology and Intellectual Property*, 6 (2007), 73-88.
- [2] Arendt, H. *The Human Condition*. University of Chicago Press, Chicago, 1958.
- [3] Bankston, K. Facebook’s new privacy changes: the good, the bad and the ugly. *Electronic Frontier Foundation*, <http://www.eff.org/deeplinks/2009/12/facebook-new-privacy-changes-good-bad-and-ugly>, 9th Dec, 2009.
- [4] Bennet, S., Maton, K. and Kervin, L. The ‘digital natives’ debate: a critical view of the evidence. *British Journal of Educational Technology*, 39(5) (2008), 775-786.
- [5] boyd, d. *Taken Out of Context: American Teen Sociality in Networked Publics*. PhD thesis, University of California, Berkeley, 2008.
- [6] Cate, F.H. *Privacy in the Information Age*. Brookings Institution, Washington DC, 1998.
- [7] De Laat, P.B. Online diaries: reflections on trust, privacy, and exhibitionism. *Ethics and Information Technology*, 10 (2008), 57-69.
- [8] Etzioni, A. *The Limits of Privacy*. Basic Books, NY, 1999.
- [9] Goffman, E. *The Presentation of Self in Everyday Life*. Doubleday Anchor, Garden City, NY, 1959.
- [10] Goldberg, I. Privacy-enhancing technologies for the Internet III: ten years later. In Acquisti, A., Gritzalis, S., Lambrinouidakis, C. and De Capitani di Vimercati, S. (eds.), *Digital Privacy: Theory, Technologies and Practices*. Auerbach Publications, Boca Raton, 2008, 3-18.
- [11] Johnson, B. Privacy no longer a social norm, says Facebook founder. *Guardian*, 11th Jan, 2010.
- [12] Joinson, A.N. and Paine, C.B. Self-disclosure, privacy and the Internet. In Joinson, A., McKenna, K., Postmes, T. and Reips, U.-D. (eds), *The Oxford Handbook of Internet Psychology*. Oxford University Press, Oxford, 2007, 237-252.
- [13] Karyda, M. and Kokolakis, S. Privacy perceptions among members of online communities. In Acquisti, A., Gritzalis, S., Lambrinouidakis, C. and De Capitani di Vimercati, S. (eds.), *Digital Privacy: Theory, Technologies and Practices*. Auerbach Publications, Boca Raton, 2008, 253-266.
- [14] Lenhart, A. and Madden, M. *Teens, Privacy and Online Social Networks: How Teens Manage Their Online Identities and Personal Information in the Age of MySpace*. Pew Internet and American Life Project (2007), http://www.pewinternet.org/~media/Files/Reports/2007/PIP_Teens_Privacy_SNS_Report_Final.pdf.

- [15] Lipton, J.D. Mapping Online Privacy. Case Western Reserve University School of Law, Case Research Paper Series in Legal Studies Working Paper 09-24 (2009).
- [16] Manes, S. Private lives? Not ours! PCWorld, http://www.pcworld.com/article/16331/private_lives_not_ours.html, 18th April, 2000,
- [17] McArthur, R.L. Reasonable expectations of privacy. *Ethics and Information Technology*, 3 (2001), 123-128.
- [18] Mill, J.S. On liberty. In *On Liberty and Other Essays*. Oxford University Press, Oxford, 1991 1-128.
- [19] Nussbaum, M.C. *Hiding From Humanity: Disgust, Shame and the Law*. Princeton University Press, Princeton, 2004.
- [20] O'Hara, K. A General Definition of Trust. Technical report, University of Southampton, <http://eprints.ecs.soton.ac.uk/18322/>, 2009.
- [21] O'Hara, K. and Shadbolt, N. The Spy in the Coffee Machine: The End of Privacy As We Know It. Oneworld, Oxford, 2008.
- [22] O'Hara, K. and Shadbolt, N. Privacy on the Data Web. *Communications of the ACM*, 53(3) (March 2010), 39-41.
- [23] O'Hara, K., Tuffield, M.M. and Shadbolt, N. Lifelogging: privacy and empowerment with memories for life. *Identity in the Information Society*, 1 (2008), 155-172.
- [24] Palfrey, J. and Gasser, U. *Born Digital: Understanding the First Generation of Digital Natives*. Basic Books, New York, 2008.
- [25] Rosenberg, H. and Feldman, C.S. *No Time to Think: The Menace of Media Speed and the 24-Hour News Cycle*. Continuum, New York, 2008.
- [26] Rössler, B. *The Value of Privacy*. Polity Press, Cambridge, 2005.
- [27] Schoeman, F.D. *Privacy and Social Freedom*. Cambridge University Press, Cambridge, 1992.
- [28] Sennett, R. *The Fall of Public Man*. Alfred A. Knopf, New York, 1977.
- [29] Solove, D.J. *The Future of Reputation: Gossip, Rumor and Privacy on the Internet*. Yale University Press, New Haven, 2007.
- [30] Solove, D.J. *Understanding Privacy*. Harvard University Press, Cambridge MA, 2008.
- [31] Strandburg, K.J. Surveillance of emergent associations: freedom of association in a network society. In Acquisti, A., Gritzalis, S., Lambrinouidakis, C. and De Capitani di Vimercati, S. (eds.), *Digital Privacy: Theory, Technologies and Practices*. Auerbach Publications, Boca Raton, 2008, 435-457.
- [32] Walden, I. Privacy and data protection. In Reed, C. and Angel, J. (eds.), *Computer Law: The Law and Regulation of Information Technology*, 6th edition. Oxford University Press, Oxford, 2007, 459-504.
- [33] Warren, S.D. and Brandeis, L.D. The right to privacy. *Harvard Law Review*, 4 (1890), 193-220.
- [34] Žižek, S. Cyberspace, or, the unbearable closure of being. In *The Plague of Fantasies*, Verso, London, 1997, 127-167.