



The Seven Veils of Privacy

Kieron O'Hara • University of Southampton

Privacy is very important. Whatever it is. The debate on privacy is notable for the lack of agreement – what is it for, is it a good or a bad thing, a right or a preference? As philosopher Judith Jarvis Thomson put it, “Perhaps the most striking thing about the right to privacy is that nobody seems to have any clear idea of what it is.”¹ In a classic legal paper, William Prosser dismissed it as a set of interests “which are tied together by the common name, but otherwise have almost nothing in common except that each represents an interference with the right of the plaintiff ... ‘to be let alone.’”² One of the most distinguished current commentators, Daniel Solove, pronounced that it was “a concept in disarray.”³

Does this matter to anyone but a philosopher, a lawyer, or a nut who doesn't want his or her data to help humanity? It does: privacy has a role to play in our psychological well-being and the health of our democracies. Being undefined doesn't stop it playing that role, but the lack of definition opens up space for critics and skeptics with different priorities. Jeff Jarvis writes that instead of coherence he sees “a confused web of worries, changing norms, varying cultural mores, complicated relationships, conflicting motives, vague feelings of danger with sporadic specific evidence of harm, and unclear laws and regulations made all the more complex by context.”⁴ In short, he's saying it's a *mélange* that shouldn't stand in the way of social progress, and that we should ignore inchoate privacy concerns and reap the benefits of sharing data with nary a backward glance. Maybe he has a point.

Do You Know What It Is Yet?

Jarvis' observation about the confusion is on the money, but we could get closer to some kind of consensus if we could leave the worries, norms,

mores, and vague feelings behind, and then perhaps conduct a more sensible conversation. If you and I are addressing only a vague feeling of danger, then we shall not get far; we'll devise a set of vague solutions. If, on the other hand, you and I have a vague feeling of danger about something relatively concrete about whose limits we agree to some extent, then our discussion would be more productive, the solution set more coherent, and the costs and benefits clearer.

So there's mileage in thrashing this out. The first question is why it's so difficult. I think it's because we're having too many conversations simultaneously that ought to be separate – the result is cacophony, category error, and people talking past each other.

For example, one influential definition of privacy as “the freedom from unreasonable constraints on the construction of one's own identity,”⁵ bundles up three separate ideas: a state in which a person is free of something (fine); freedom from unreasonable things, so necessarily a good thing for the individual, and plausibly something that should never be breached (since unreasonable things shouldn't happen if they can be prevented); and the construction of identity.

Yet privacy is sometimes breached for good reasons, and half the arguments about it are about how we identify those circumstances and legislate for them. Indeed, many cultures see privacy as a bad thing – privacy-related terms in ancient Greek (*idiotes*) and Latin (*privare*) had negative, not positive, connotations. And sometimes, privacy is a state in which someone has no interest in identity – that person just wants to get away from the madding crowd, or watch the ball game with a beer. The authors crammed contentious things about privacy into the above definition, and for good measure smuggled in their own opinions about what it is for. If someone denied,

say, that privacy was required for identity, the debate would degenerate into the semantics of the definition, rather than remaining substantive and concerned with the application of an agreed (if contested) concept.

The Seven Veils

We can approach privacy at a number of levels, and failure to recognize this ushers in the confusion and ambiguity that we find in writing on the topic. These levels conceal the roots of disputes and agreements, and veil the nature of privacy itself. Had there been six or eight levels, I couldn't have used my catchy title, but there are seven, so here's to agreeable serendipity.

Level 1: conceptualization and realization. Underlying everything, there's a concept. This can't be simple; there are probably several of them in parallel. We know privacy varies across cultures, and that new technologies – writing, the portable camera, digital data storage, the Internet – create new problems. The first caveman to chisel a hole in his cave wall probably divided Neolithic opinion between those who welcomed the extra light and ventilation, and those who shook their heads and grunted about the shocking privacy implications.

For now, let's note that privacy takes many forms. It can be epistemological (Bob shouldn't acquire information about Alice), decisional (Bob shouldn't interfere with Alice's actions), spatial (Bob shouldn't intrude into Alice's space), ideological (Bob should tolerate Alice's beliefs), and economic (Bob shouldn't appropriate, use, or exchange Alice's property). All of these, particularly the first, have implications for online behavior. They are all states – Alice has her privacy when she is able to act freely, when her space is without a trespasser, when her data aren't being processed.

Do they have anything in common? Perhaps. Let's settle, for now, for the importance of a boundary. Bob crosses a

line, metaphorically or otherwise, when he breaches Alice's privacy. And at any time a new type of behavior or technology can erect a new privacy boundary.

You can plug your own pet theory about privacy into level 1; I have my own views (detailed in the "Privacy at Level 1" sidebar), but they aren't essential to the six levels that follow. What I want to argue is that conceptual ambiguity resides here. The vague worries, changing norms, and complex relationships that concern Jarvis are distributed across the other six levels of discourse.

Level 2: empirical facts. Given a particular concept of privacy, then in principle, if not always easily, it's a simple matter to check whether someone actually has their privacy in this respect, or whether the line has been crossed. Either there's someone's eye at the spyhole into Alice's bathroom, or there isn't. Either someone is in possession of Alice's personal data, or no one is.

Privacy may occur because of someone trying to be private, but equally it might be unchosen, accidental, unnoticed, compulsory, or involuntary.⁶ It may be given away freely or sold. Different concepts may come into play at the same time – an individual may be private in some respects but not others. A person may be private as part of a group, but not be private within that group.

Level 3: phenomenology. This is a level often missing from discussion. A particular privacy situation will feel like something to Alice, and the way it feels will influence how tolerable she finds the state. Note that the empirical facts of Alice's privacy needn't be known to her.

Privacy isn't a matter of perception, but perception matters to the actions someone takes to preserve, or not preserve, his or her privacy. Alice showering unobserved, and Alice showering with Bob's eye at the spyhole feel identical to Alice; the phenomenology is unchanged, yet the privacy situation is radically different. Similarly, the

phenomenology of privacy is culturally and contextually variable. Compare taking off clothes: with no observer; in front of your partner; in front of your mother; in the foyer of the Waldorf Astoria; on stage before a hundred people for a fee; on a nudist beach; in front of your doctor; in the dorm room for a bet; or at the behest of a zealous customs inspector. It's the same action in each case, but a very different feeling.

If we happen not to care about a privacy breach, then there's no reason even to notice it. Solove writes that "we are frequently seen and heard by others without perceiving this as even the slightest invasion of privacy."³ True, but that just means that it's unimportant. We aren't private, in the relevant respect, when being seen and heard by others, whether we care, and whether we notice.

E-commerce and social networking sites work hard at this level in their service provision.⁷ Social networkers feel private as they share information and chit-chat with their small group of friends. It feels warm and social, not like the chit-chat is owned by the network. Even if a social network is open about its use of information, via its privacy policy, and its users cognizant of the widespread exploitation of their personal data in the advertising business, that doesn't mean that social networking will feel as if it is exploited by advertisers and site owners.

Level 4: preferences. Given Alice's perceptions of privacy and her feelings about it, she will have certain preferences for or against it. She may prefer to be private in her dealings with the church, but online may prefer to be visible to her network. She will have preferences about other people's privacy – she may wish to keep her children's digital footprints as small as possible, for example. She may not want Bob to tell her all his troubles – she wishes he were more private. Preferences vary widely between individuals and across contexts for the same individual, and

Privacy at Level I

The characteristics of privacy have only been sketched. Indeed, this may be all that can be done if the concept itself suggests no more than a family resemblance.¹ The framework of seven veils sketched here is a modular structure — if you have your own pet theory of privacy (and there are plenty of them), you can just plug it in at level I. As long as your theory takes privacy as a state, and not a right, preference, norm, or legal concept, then the framework will separate the facts of privacy from our individual and social attitudes to it.

Is there more to say about what goes on at level I? How do we recognize a concept of privacy when, for example, new technology or new practices emerge?

I think much has to do with the psychology of ownership. By this, I absolutely do not mean property ownership in a legal sense, or even in John Locke's sense of "every man [having] a property in his own person."² I mean ownership as signaled by a compulsion to use possessive adjectives — my face, my body, my information, our beliefs, my space, our house, my name. "This is my business" means keep your nose out (your nose is your business, of course). This is a basic social instinct, and our legal ideas of property ownership are derivative from it. If I say "this is my business," I might be referring to my hairstyle, my beliefs about Donald Trump, the way I discipline my children, or the number of cigarettes I smoke on average per day; I own none of these, and can't sell them or leave them in my will.

Compare that to the notion of this is my house, but I don't own it (I rent it). This is my information, but I don't have any rights over it (Facebook has the rights, but it's still, in this non-legal sense, my data, because it's about me). Suppose Alice has a prosthetic leg; in that case, having bought it, she probably is the legal owner of the limb, yet she has a different, more profound sense of ownership of her real leg. I refer to ownership in the latter sense. Note that such adjectives may define an individual's private sphere, or that of a group. These are my friends (so that we have a collective privacy interest); I don't own them, and can't sell them to a passing slave trader.

The feeling of ownership is a deep component in the construction of one's identity, the self, although there are many competing ideas as to how that might function.^{3,4} Ownership implies some kind of central and exclusive interest, or a privileged position. Alice gets to decide who enters her house (even if she doesn't legally own it). Alice decides who uses or disposes of her material possessions. Alice decides whether and when to reveal her body, or (in many cultures) her face,⁵ or her name. The privilege may only be conceptual: Alice's information is about Alice, and if it's

not about her it's not her information. As noted, she may not be able to defend these privileges without the cooperation of her fellows, but her privileged position is socially accepted.

Sometimes the privileged position is more nominal than effective. Private information about Alice may be unknown to her, and may be shared by others; but in most cultures, including Western liberal democracies, there are some taboos that protect privacy without her knowledge. Even the controversial US third-party doctrine,^{6,7} under which information disclosed to third parties isn't defended by the US Constitution's Fourth Amendment against unreasonable searches, implies that the subject must take the first step in stripping away the legal protections. The doctrine is also founded on the individual's (and no one else's) "reasonable expectations of privacy."

Ownership, in this non-legal sense, subtends a boundary. There are my/our business, feelings, states, and decisions, and then there are bits of business, feelings, states and decisions that aren't mine/ours, over which society recognizes none of my/our privileges. The taxman may probe the financial affairs of many people, but only Alice's financial affairs affect her privacy.

A breach of privacy crosses a boundary, or challenges a privileged position. It implies attention towards some aspect of private behavior or position (Jed Rubenfeld writes of an "unarmed occupation of individuals' lives" — a good phrase, although he focuses on privacy invasions by government).⁸ Boundaries, (non-legal) ownership indicated by use of first-person possessive adjectives, and freedom from attention are all important indicators that privacy concepts are in place.

References

1. D.J. Solove, *Understanding Privacy*, Harvard Univ. Press, 2008.
2. J. Locke, "Second Treatise," *Two Treatises on Government*, Cambridge Univ. Press, 1988, pp. 265–428.
3. J. Dokic, "The Sense of Ownership: An Analogy between Sensation and Action," *Agency and Self-Awareness: Issues in Philosophy and Psychology*, J. Roessler and N. Eilan, eds., Oxford Univ. Press, 2003, pp. 321–344.
4. S. Gallagher, *How the Body Shapes the Mind*, Oxford Univ. Press, 2005.
5. F. El Guindi, *Veil: Modesty, Privacy and Resistance*, Berg, 1999.
6. O.S. Kerr, "The Case for the Third-Party Doctrine," *Michigan Law Rev.*, vol. 107, 2009, pp. 561–601.
7. E. Murphy, "The Case against the Case for Third-Party Doctrine: A Response to Epstein and Kerr," *Berkeley Technology Law J.*, vol. 24, no. 3, 2009, pp. 1239–1253.
8. J. Rubenfeld, "The Right of Privacy," *Harvard Law Rev.*, vol. 102, 1989, pp. 737–807.

needn't be consistent. We need to be careful to separate the facts of privacy from our concern about it. Ruth Gavison argues that "our interest in privacy ... is related to our concern over our accessibility to others."⁸ That's true, but

our interest being related to the concern doesn't make our concern part of the concept. Alice may be private or in a breach of privacy, while having no preference about it. She may make a fuss when her preferences aren't satisfied,

and may only take note of privacy when it's problematic, but that doesn't mean that its being problematic is part of the concept.

Much of the discussion so far has been psychological, about the self. Yet

now a social element emerges, because society has preferences about the privacy of individuals, too. Alice may wish to keep her financial details private, but the Internal Revenue Service, for perfectly good reasons, wants to see them (and were Alice Swedish, her society would wish her not only to give up the details to the taxman, but also to expect them to be published online). Alice doesn't want the police to have access to her heating bills, but — if she's growing marijuana in her attic — they may have grounds to seize them. Pace commentators such as Amitai Etzioni,⁹ however, it's not always the case that individuals like Alice benefit from their privacy while society benefits from transparency and exposure.¹⁰ Alice may prefer to sell her vote, but society wishes her to make her decision as to who to support privately. Alice may anticipate a life of partying, but society prefers her to care for children for whom she is responsible in her domestic sphere. Sociologist Irwin Altman described the endless process of negotiation of the boundaries between individuals, groups, and society, and this is no less apposite in the digitally networked age.¹¹

Level 5: norms. Without assuming a naïve linear route through the levels, when sufficiently many people share similar preferences, we might expect these preferences to ossify into norms, expectations, conventions, and regularities of action and attitude. If Alice admonishes Bob to block up the spyhole because she doesn't like it, that's a level-4 claim. But if she admonishes Bob because spying on others is not the thing done around here, then she has moved to level 5. Helen Nissenbaum's theory of contextual integrity sits at this level.¹² She argues, for instance, that when considering putting some process online, someone should consider the norms that apply in the offline process (for instance, who gets to see customer information in a commercial transaction), and

ensure that those norms are respected online, thereby preserving the situation's contextual integrity.

Level 5 normative aspects of privacy aren't part of the concept. Solove writes that “few would contend that when a crime victim tells the police about the perpetrator, it violates the criminal's privacy,”³ but actually it does exactly that. And a good thing, too — the norm in that case works against privacy, for good social reasons. Privacy is about whether the details of someone's behavior are passed on; we need to separate the empirical question about what has happened from the normative one about what ought to have happened.

Social norms are vital for the protection of privacy, and explain much of its cultural diversity. They allow people to pursue their preferences (when preferences and norms are congruent) without needing to establish control. For instance, if Alice wants to mark out her personal space, all she needs is a little picket fence around her property; remarkably few people will be minded to cross it, although there's nothing physical to stop them.

Norms also influence the management of privacy with other concepts and mechanisms. Alice might give up privacy, for example, by discussing something personal with her doctor. In return, she expects confidentiality (that is, that her confidence won't leave the medical system).

Level 6: law. Norms can be formalized by turning them into laws or regulations, making the normalized behavior not only conventional but compulsory. This can have the effect of moving us from an adaptable, understandable, and context-sensitive norm to a more rigid, less-intuitive rule.¹³ Equally, laws can be devised to extinguish or create norms.

A law requires more than mere social agreement, and so we move beyond civil society towards a notion of governance, and the application of sanctions by a state. Privacy law is important in understanding firms' and

governments' practice with personal data, but the legal level has a hegemonic tendency — discussions about privacy tend to become discussions of law. We must remember that privacy isn't a legal concept, even though (in some countries) some types of privacy breach are illegal or actionable. One aim of a (level 6) law is to enable as many citizens as possible to satisfy their (level 4) preferences. At level 6, Alice can take legal action against Bob for his use of the spyhole, allowing her to satisfy her privacy preference for showering without an audience; at level 5, she can only appeal to social conventions.

Level 7: rights. Finally, privacy has moral and ethical connotations. It has political worth (for example, Beate Rössler argues that privacy supports individuals' autonomy, vital for the functioning of liberal democracy).¹⁴ At level 7, Alice can argue that Bob is morally wrong to spy on her in her bathroom. We go beyond socially endorsed notions of what's right and wrong, to questions of value, logic, and conceptual analysis, separate from the other six levels, yet bringing us back to the conceptual evolution that characterizes level 1.

Views of rights vary. A legalist position, prominent in classic works by American scholars (such as Samuel Warren and Louis Brandeis¹⁵ and Prosser²) is that we can “read off” our rights as a generalization, or a direction of travel, detectable in law (for example, in the US Constitution). The common law roots of US law locate much of this in financial or reputational harms that people have taken to court. In the EU, the position is somewhat different; universal rights are made explicit in treaties and documents, and laws enacted in Europe are expected to respect them. A court judges whether there's a conflict. The issue for lawyers and philosophers is whether, for example, a social network selling Alice's personal data to a third-party advertising broker intrudes so far into the private sphere that it threatens her private life.

Across the Levels

If we're discussing privacy, then it helps — actually, it's vital — not to jumble these levels. Suppose we're considering whether there's a right to privacy. Much will depend, for example, on whether the right protects the individual (like the right to life) or the collective (like the right to an open trial). Yet we can't have that discussion if we've written the presumed benefits into the definition of privacy in the first place. And if indeed we've done that, then we'll be shocked to discover that there are people in the world who don't care much about it. Our response may then be that such people are unaware of the issues, or have some kind of cognitive dissonance (the so-called *privacy paradox*). Yet it may actually be that such people just don't care much to be in that kind of state, and would dispute the nature of the supposed benefits.

There are causal links between truths at the different levels, but we shouldn't generalize too much about their direction. One common sense type of reasoning will take us up through the levels — some particular type of privacy feels good or right to Alice (level 3), so she prefers it (level 4), as do many of her fellow citizens, leading to expectations or conventions emerging (level 5), which may at a later date be valorized in regulation (level 6), from which we abstract to create a right (level 7).

But the links may go in the opposite direction, or skip levels. Bob doesn't want to be spied upon (level 4) because it's just not done in his society (level 5), not the other way around. The sale of Alice's personal data annoys her (level 3), because she has a right to her privacy (level 7). There are norms in many cultures (level 5) which are designed to make individuals feel private (level 3); Mireille Hildebrandt writes of Japan, where, despite paper-thin walls in houses, people behave as if they're unaware of private conversations that they must have overheard,¹³ while Robert Murphy writes that in

communal living areas in some cultures, people simply avert their gaze from other people's space.¹⁶

Mention of norms reminds us that control — often assumed as a factor in defining privacy¹⁷ — is secondary context, not a first-order facet of the concept. Alice may be able to protect her privacy herself (by destroying evidence of an event, perhaps), or she may use the law (by suing trespassers), or exploit social norms (by putting a small fence around her property), or she may be granted her privacy by the people around her. Only in the first case does she have total control, and she may feel less secure in her privacy as we go down the list. Self-determination often remains where control is ineffective, but beyond that, privacy may be conferred by a person's fellows.

If we can keep the question of whether someone actually has privacy free of value-related discourse, we might be able to unpick the different questions about the psychology, sociology, law, and morality of privacy. Tangling them up is a route to bafflement.

If, for example, you think that privacy is by definition a good thing or even a human right (a level 7 thing), then your definition will be complicated by an evaluation of the goodness or rightness of what you define. You may be thrown by the fact that, for example, in digital contexts, few people seem to be bothered by the loss of this good. On the other hand, if you decide that privacy is located in norms of concealment and exposure (a level 5 thing), you might agree with Mark Zuckerberg (who of course has no axe to grind in this area), that it's a thing of the past, as evidenced by the fact that a billion people are quite comfortable giving all their information to, er, Mark Zuckerberg.¹⁸

So how does this affect the digital citizen's experience of privacy and its lack? My aim is to separate the effects and affects of privacy from the facts.

Privacy is too often defined as a good thing (and then it's a mystery why people give it away). It's often defined as law (so we have to go to court to find out how much of it we deserve). Sometimes it's defined as control (so we don't have very much of it). Removing these complicating factors from the simple state in which a boundary is crossed or not enables us to think about when that's problematic, and why this differs not only across cultures, but also across generations and even for the same individuals.

This framework of the seven veils won't solve the myriad philosophical and political difficulties of privacy. It won't divulge whether the EU is right or wise to count privacy as a right, nor whether the US is right to insist that privacy protections in law should be triggered by harms.¹⁹ It does tell us that privacy goes wider than whatever we have a right to, and that privacy breaches needn't be (and usually aren't) accompanied by harm, whether financial or reputational.

Post-Snowden, security services have argued that bulk collection of data doesn't breach privacy — only analyzing it counts as surveillance. We can now see that collecting and analyzing are two different types of breach of privacy (level-1 concepts, the difference between them being the amount of attention paid to the data), and the first one may have few effects on the data subject (data collection will usually be completely invisible at the phenomenological level 3). The effects of data analysis and profiling may be evident to the data subject (she may be denied a seat on an airplane), but she may not associate those effects with a privacy breach. And if we ascend to level 6, we can ask the separate question about whether bulk collection is legal.

The framework tells of the importance of affective design in, say, social networks or e-commerce.⁷ The way an experience of (breach of) privacy feels, or is concealed, will change the phenomenology and preferences of

individuals, which may result in behavior that apparently shows a disregard on their part of assumed norms. For instance, after a profiling scandal in which the supermarket chain Target discovered that a teenager was pregnant before her parents did, “we started mixing in all these ads for things we knew pregnant women would never buy, so the baby ads looked random. ... As long as we don’t spook her, it works.”²⁰ That’s level-3 thinking, indeed. The seven-level framework encourages us to tease the different levels apart, and to consider that the individual’s understanding of the situation may not include the recognition that a particular privacy norm is operative in the context in which he finds himself.

Indeed, we might even be able to unpick the so-called privacy paradox,²¹ which suggests that individuals are irrational or lack self-knowledge when their behavior transgresses their stated privacy preferences. Perhaps people do adhere to particular norms at level 5, but their level-4 preferences are concerned with a whole Gestalt, crafted by system interface designers to affect them at level 3, involving much more than a simple experience of a privacy breach or otherwise. Any norm, including those of privacy, will be disregarded if the context makes it appropriate to do so. The privacy paradox isn’t such a paradox when we see how easy it is to put people into situations where privacy doesn’t seem like such a big deal. □

Acknowledgments

This work is partly supported by SOCIAM: The Theory and Practice of Social Machines, funded by the UK Engineering and Physical Sciences Research Council (EPSRC) under grant EP/J017728/1. Many thanks to Mark Elliot of the University of Manchester for several stimulating conversations about this article’s topic.

References

1. J.J. Thomson, “The Right to Privacy,” *Philosophy and Public Affairs*, vol. 4, 1975, pp. 295–314.

2. W.L. Prosser, “Privacy,” *California Law Rev.*, no. 48, 1960, pp. 338–423.
3. D.J. Solove, *Understanding Privacy*, Harvard Univ. Press, 2008.
4. J. Jarvis, *Public Parts: How Sharing in the Digital Age Improves the Way We Work and Live*, Simon & Schuster, 2011.
5. P.E. Agre and M. Rotenberg, *Technology and Privacy: The New Landscape*, M.I.T. Press, 2001.
6. D.M. O’Brien, *Privacy, Law and Public Policy*, Praeger, 1979.
7. F.N. Egger, “Affective Design of E-Commerce User Interfaces: How to Maximise Perceived Trustworthiness,” *Proc. Conf. Affective Human Factors Design*, 2001, pp. 317–324.
8. R. Gavison, “Privacy and the Limits of Law,” *Yale Law J.*, vol. 89, 1980, pp. 421–471.
9. A. Etzioni, *The Limits of Privacy*, Basic Books, 1999.
10. K. O’Hara, “Are We Getting Privacy the Wrong Way Round?” *IEEE Internet Computing*, vol. 17, no. 4, 2013, pp. 88–92.
11. I. Altman, *The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding*, Brooks/Cole, 1975.
12. H. Nissenbaum, *Privacy in Context: Technology, Policy and the Integrity of Social Life*, Stanford Law Books, 2010.
13. M. Hildebrandt, *Smart Technologies and the End(s) of Law*, Edward Elgar, 2015.
14. B. Rössler, *The Value of Privacy*, Polity Press, 2005.
15. S.D. Warren and L.D. Brandeis, “The Right to Privacy,” *Harvard Law Rev.*, vol. 4, 1890, pp. 193–220.
16. R.F. Murphy, “Social Distance and the Veil,” *Am. Anthropologist*, vol. 66, 1964, pp. 1257–1274.
17. A.F. Westin, *Privacy and Freedom*, Atheneum, 1967.
18. I. Paul, “Facebook CEO Challenges the Social Norm of Privacy,” *PCWorld*, Jan. 2010; www.pcworld.com/article/186584/facebook_ceo_challenges_the_social_norm_of_privacy.html.
19. D. Solove, *Privacy and Data Security Violations: What’s the Harm?* 25 June 2014; www.linkedin.com/pulse/20140625045136-2259773-privacy-and-data-security-violations-what-s-the-harm.
20. C. Duhigg, “How Companies Learn Your Secrets,” *New York Times*, 16 Feb. 2012;

www.nytimes.com/2012/02/19/magazine/shopping-habits.html?_r=0.

21. S.B. Barnes, “A Privacy Paradox: Social Networking in the United States,” *First Monday*, vol. 11, no. 9, 2006; <http://firstmonday.org/ojs/index.php/fm/article/viewArticle/1394>.

Kieron O’Hara is a senior lecturer and a principal research fellow in the Web and Internet Science Group in the Electronics and Computer Science Department at the University of Southampton. His research interests include trust, privacy, open data, and Web science. O’Hara has a DPhil in philosophy from the University of Oxford. Contact him at kmo@ecs.soton.ac.uk.

cn Selected CS articles and columns are also available for free at <http://ComputingNow.computer.org>.



It’s already at your fingertips

Computing in Science & Engineering (CISE) appears in the IEEE Xplore and AIP library packages, so your institution is bound to have it.

