Laura Huey
University of Western Ontario, Canada. lhuey@uwo.ca

Welcome to the inaugural run of Surveillance & Society’s new debates/discussion section!

We have launched this new section in order to promote the exchange of ideas and discussion of relevant topics among readers. To that end, each year we will invite a group of discussants to contribute papers in a selected topic area to be published annually in the December issue. These papers are intended as means of stimulating readers to respond with their own thoughts, in the form of commentaries we will seek to publish in future issues within the year following.

To help us get started, we invited discussants from various fields, who kindly agreed to respond to one or more of three questions we posed to orient the discussion. This year’s panel of invitees is:

- danah boyd, Microsoft Research
- Steven T. Margulis, Grand Valley State University and Gary T. Marx, M.I.T.
- Judith Rauhofer, University of Edinburgh
- Paul Rosenzweig, Red Branch Consulting and George Washington University
- Micheal Vonn, BC Civil Liberties Association
- Reg Whitaker, York University and the University of Victoria

Our focus for this year is “The Future of Privacy Online: Three Questions.” Why the future of online privacy? Given that there has been much recent debate on the future of online privacy within academic and policy-making circles, as well as among members of the general public, we thought it would be an illuminating exercise for readers if we were to ask contributors from different fields, and with different perspectives, to share their views on what we see as three important questions. These questions are:

In relation to online privacy ...

i) Where are we?
ii) What should the future look like?
iii) And what is the best means of acquiring that future?

We also asked participants to address their response by selecting one of three areas:

- social media,
- other forms of information technology, and
- national security.
We received six commentaries with six unique views on the questions posed. Three of our invited authors opted to tackle some of the thorny issues that arise in discussions of privacy and national security in the online context. Surveying the landscape of online privacy in the post 9/11 world, Micheal Vonn says those individuals and groups who support traditional notions of privacy are in “deep sh**” because of the speed at which privacy-piercing technologies proliferate, and the haste with which governments and other actors attempt to exploit them. However, Vonn is not ready to throw in the towel. Instead, she is issuing a rallying cry, one founded on the belief that privacy is not dead, it just needs a make-over: “we need a new model and understanding of privacy that gives this value its appropriate weight culturally, legally and constitutionally.” Reg Whitaker is also taking stock of the digital environment post-9/11 and similarly appears to not like what he sees: a series of Western governments that have enacted privacy invasive legislation, frequently with little or no consultation or justification for measures taken. Whitaker notes one interesting exception: Canada. Tracing the history of Canada’s efforts to pass legislation that would similarly provide security agencies with enhanced data-tapping and other online investigative powers in the face of substantial public opposition, what is revealed is—potentially—a model of resistance for other nations. Taking an entirely different tack, Paul Rosenzweig wants to solve what is often viewed as an intractable problem by policy-makers: the privacy-security zero sum game in which any move to increase or decrease online privacy or other freedoms is met with a commensurate increasing or decreasing of public security. For Rosenzweig, this zero sum game occurs because we treat privacy as an absolute rather than instrumental right. He suggests that we should move away from viewing privacy as being synonymous with anonymity and instead reconceive it as a limitation on consequence, paying greater attention to “the means/ends/consequence fit of any proposed dataveillance program.”

Focusing on information technology more generally, danah boyd also believes that it is time for a change in our approach to understanding privacy. For boyd, liberal democratic conceptions of privacy as an individual right do not work well within networked societies. In essence, she argues that to the extent that most of us do not “bowl alone” in the online world, we need to shift towards models of privacy that “position networks, groups, and communities at the center of our discussion.” Stephen Margulis and Gary Marx have also opted for an examination of information technology—in particular, they explore e-commerce in the U.S. and what social science research has to tell us about the treatment of privacy concerns online. Summing up this body of research, the legislative history of an assorted number of proposals in the U.S. Congress, various voluntary privacy-enhancing schemes and their limitations, these authors conclude that it is likely that the protection of consumers’ privacy will remain in the hands of the private sector and, in particular, those of consumers. Thus, their warning: “caveat emptor.” Judith Rauhofer is not satisfied with the caveat emptor approach. One reason for her dissatisfaction is that, as she notes, the current economic crisis too easily allows e-businesses to claim privacy-infringing data collection practises as economic necessity and thus trump lesser considerations, such as consumer privacy rights. As she puts it, “at a time of global recession, the economic imperative has therefore joined ‘national security’ as the public policy objective of choice to which individuals’ privacy is expected to take a backseat.” To help stop our current “race to the bottom,” she too is suggesting a shift in perspective: away from “the existing defensive discourse around data protection” toward a multi-pronged “positive agenda for privacy” that includes social normative, technological and public policy components.

Now that we have the ball rolling in the form of the thought-provoking contributions that follow, we invite interested readers to consider participating in the forum by responding to, elaborating on, or otherwise contributing their own thoughts and ideas on this topic. Responses should be in the form of a “comment” that addresses the content of a given piece and is thus of no more than 3-5 pages double-spaced in length. Please send your comments to the Debates Editor, Laura Huey (lhuey@uwo.ca). These will be reviewed by her upon submission, and she may seek revisions concerning any typos, spelling/grammar, unclear language or unsuitable content.
Micheal Vonn
BC Civil Liberties Association, Canada. micheal@bccla.org

Question 1: Where Are We? — Sanitation Engineering Suddenly Very Sexy

Simon Davies, one of the world’s foremost privacy experts, used to say that privacy advocates are the sanitation engineers of civil liberties: we don’t have a very sexy job, but boy-howdy, is it important. While once a true portrait, this is no longer quite as apt because privacy is increasingly becoming sexy. On one side of the ledger, this is an exciting development. Ordinary, non-policy-wonk people are increasingly voicing concerns about privacy and surveillance, especially in the online context. This shift is in part a success of increased education and advocacy. But in the main, this heightened awareness and engagement is a reflection of how dire things have become. We are reaching a crisis point that is increasingly palpable. In other words, ‘sanitation engineering’ is suddenly sexy because people are starting to understand in a big way that we are in deep sh**.

New forms of surveillance and what some are calling ‘the battle for the free internet’ are key issues in a broader crisis about the state of our democracy. At a gallop since 9/11, we have seen the democratic formula turned upside down with citizens increasingly transparent and accountable to government and government increasingly secret and insulated from accountability to citizens. When we think about how the internet can be and is being turned into a tool for surveillance and control, we no longer think only of ‘those’ places, elsewhere, with authoritarian regimes.

When we look to the Kremlin’s new internet surveillance program that involves a single register of banned websites and a new system allowing ISP’s not only to filter traffic, but to monitor it on a nationwide scale, no one is buying the cover story that this is (only) a program to detect child pornography. The ramifications for all forms of political speech are only too apparent. And this is finally coming home to us in the so-called advanced democracies: virtually all governments are keen to censor the web and monitor citizens. For a temperature-taking, see the U.K.’s draft Communications Data Bill, which involves blanket collection and retention of all online data. As Privacy International pointed out in its submission to the U.K. Parliament, the technology that would be used is currently only deployed in Kazakhastan, China and Iran.

While many countries, including Canada, are looking to expand government’s reach into the personal information of citizens through ‘lawful access’, there is also the vast, nebulous terrain of what is happening to our information via covert operations of highly dubious lawfulness. We know, for example, that the U.S. Total Information Awareness program has been resurrected by the NSA, which is building a one million square foot facility in the Utah desert to store and process massive amounts of the world’s communications. This program includes a crucial code-breaking component for heavily encrypted
information, such as legal documents, diplomatic and military communications, and financial information. The upshot would appear to be that anything they can capture and crack is up for grabs.

And, of course, what exactly is up for grabs is completely unprecedented because the new surveillance is not only about the internet of communications, but also about meta-data (even our data has data) and increasingly also about the internet of things. We expect something like 15 billion internet-connected devices by 2015, with about one third of those being part of broader ‘intelligence systems’—the idea being that scads of everyday items, from our light bulbs to our clothes, will be internet-ready to communicate with our control devices in real time.

The CIA, for one, is very excited about such developments. David Petraeus enthused about the ‘transformational effect’ on ‘clandestine tradecraft’. Of course, Petraeus has since been toppled as the director of the CIA over emails that were inadvertently discovered in a completely unrelated cyberstalking inquiry. As Marc Rotenberg of the Electronic Privacy Information Centre said regarding how cyberinvestigations sweep up huge amounts of information: ‘If the CIA director can get caught, it’s pretty much open season on everyone else’. No official word as yet about whether Mr. Petraeus is feeling less enthusiastic about transformations in ‘clandestine tradecraft’ at this juncture.

And, in addition to government-sponsored surveillance, we should also note the increasing use of spyware by ‘others’. Recently, Citizen Lab at the University of Toronto reported that commercial espionage programs, which (unsurprisingly) are used by governments to monitor activists and suppress dissidents, are increasingly also available to your run-of-the-mill cyber-criminal. Fin Fisher spyware and variants that can activate cameras and voice recorders, grab images off computer screens, tap Skype calls, remotely log keystrokes and steal files on hard drives, have been discovered on public control servers across five continents.

**Question 2: Where Do We Want to Go? — Getting the Elephant Off the Other End of the ‘Teeter Totter’**

Security concerns are real and important. That said, the rubric of ‘security’ is now a catch-all for dangerous authoritarianisms. We can no longer abide by the deeply flawed security vs. privacy paradigm where the security elephant lands on one end of the ‘teeter totter’ weighing a ton (‘public’ safety), with a sole individual on the other side claiming a ‘personal’ right of privacy. We need, among other things, to urgently understand that privacy is not pitted against the public interest: it is the public interest. Privacy is both a personal and societal value, underpinning all our democratic rights, and we need a new paradigm that reflects that.

The re-framing that we need sees privacy as relational and not spatial. As Jennifer Nedelsky (1990) sets out in the article, ‘Law, Boundary and the Bounded Self’, we use spatial paradigms to illustrate basic rights, and none more so than privacy. Property rights have deeply influenced the privacy rights paradigm in North America. We traditionally have strong privacy rights in our own bodies and our homes, but those rights peter out the farther we get from our ‘private’ space; the perverse result being that isolation is the best privacy protection. But citizens (rightly) are unwilling to sacrifice relatedness for the values of privacy and autonomy. Not because privacy and autonomy are not important, but because we’ve got the wrong model. The privacy-are-dead types are always pointing to the prevalence of social networking as evidence that people ‘don’t care about privacy’, and yet, it is consistently the digitally savvy and hyper-connected leading the charge on privacy rights (see: the Open Media campaign against Bill C-30). Our relationships and our communications are no longer spatially contained; a digitally mediated world makes nonsense of the spatial construction of privacy.
We need a new model and understanding of privacy that gives this value its appropriate weight culturally, legally and constitutionally. And on the other end of the balance beam, we have to start dismantling the undue secrecy of the security state so security claims can be realistically assessed and given appropriate consideration and weight.

While governmental non-transparency and non-accountability are vast problems, it is arguable that these democratic concerns are particularly acute in digital rights and privacy matters where secrecy and policy laundering are perennial problems. We urgently need accountability in these realms. We can no longer permit our constitutional rights to privacy and free expression to be negotiated away in secret ‘trade’ or ‘security’ deals that leave citizens and our Parliamentary representatives reliant on leaks of draft documents for any inkling of what our governments are doing ostensibly in our name. It is nearly a full time job to stay on top of all the secret deals that impact our digital and privacy rights, not to mention omnibus secret deals like Canada’s Perimeter Security Agreement with the U.S. which will have a massive impact on citizens’ privacy rights and the entire sphere of ‘cybersecurity’. This is a very aggressive ‘harmonization’ agenda, with major ramifications for our sovereignty and about which Canadians are being kept almost entirely in the dark.

Where do we need to go? Not to put too fine a point on it, we need a genuine democracy. The catch-22 is that we need our digital rights and our privacy rights to help us get there. We have to fight on several fronts all at once because they are connected.

Question 3: How Do We Get There?—Do Everything

We need technological skills and talent on the privacy side of the equation; from open source encryption, like TOR, to Eben Moglen’s work on personal servers—we need more privacy tools and we need to educate people in how to use them. We need to create and share templates that people in individual countries can use for advocacy. Right now Privacy International is doing invaluable work in developing international principles on lawful access and communications surveillance. We need threshold setting of exactly this kind. As we can see in the context of Bill C-30 in Canada, with the legislation stalled because of a public outcry, government and police supporters of the bill will be in the market for privacy advocates to help shape amendments to some of the most problematic components of the bill in order to have the revised bill declared ‘privacy community approved’. There is always tension within any advocacy community about when to stand united in opposition and when to work with policy-makers in hopes of at least making what is bad marginally better. Work to create consensus on the fundamental principles of lawful access will help ensure that advocacy efforts can stay strongly unified and are not unduly fractured.

We need strategic litigation. And we need to win it.

We need to understand that the privacy battle is genuinely non-partisan. Lessons learned from Bill C-30 include the fact that some of the most important objections to the bill came from deep within the government’s own constituency.

We need to use Freedom of Information (FOI) creatively. For inspiration, see the work of security researcher Chris Sogohain.

We need to make partnerships between advocates and academics to do the in-depth research that is needed in the privacy and security policy realm.

We need to counter simplistic homilies about ‘good guys’ [police and intelligence] and ‘bad guys’ [terrorists and criminals] that are so predictably trotted out in an argument for expanded surveillance. If Brits have recently been ‘catchin’ religion’ about privacy it has much to do with the corruption of police
and other officials discovered in the tangled web of the phone-hacking scandal, including police officers selling geo-location data gleaned from cell phones (apparently $500 a pop was the going rate).

Picking up on that…

**We need** effective oversight of all agencies empowered to conduct surveillance. This includes the newly created Canadian Cyber Incident Response Centre, which currently operates with a very vague mandate and no form of external review. This also includes implementing the national security oversight mechanism recommended by the Arar Inquiry, and needed now more urgently than ever because of the greatly increased data sharing with the U.S. called for in the Perimeter Security Agreement.

**We need** to explain to the public and policy makers how the wrong ‘security’ measure actually undermines real security. See Susan Landau’s work on how surveillance tools like intercept capability decrease the security of communications systems, like the CALEA-compliant wiretapping capabilities built into the Greek Vodofone switch that allowed some 100 senior members of the Greek government (including the Prime Minister) to by spied up by unknown parties.

And, as the late great Molly Ivins said:

**We need** to have fun while we’re fightin’ for freedom; cause we don’t always win.

**References**

We begin in the fall of 2001. In the immediate shadow of the 9/11 terrorist attack on the Twin Towers, the Canadian Parliament debated the *Anti-terrorism Act 2001*. Despite its title, this legislation was something of a mini-omnibus bill, a national security act covering a range of security issues beyond terrorism. However, there was one clearly identified gap. Unlike the *USA Patriot Act*, rushed precipitously through the US Congress, the Canadian legislation contained no provisions for enhanced electronic surveillance of internet communication. Instead, the government promised to follow up with further legislation addressing this latter issue, with a nod toward the 2001 European Convention on Cybercrime as a broad set of guidelines. The impression left by government spokespersons was that new communication technologies and a deregulated telecommunications environment required some serious legislative upgrading and modernization of electronic surveillance rules to meet the threat of terrorism and international organized crime. The expectation was that the new legislation would follow expeditiously, although there would be time for public and industry consultation before a final draft was prepared.

Fast forward eleven years to the fall of 2012. Despite two separate rounds of national consultation on what was called in Canadian Orwell-speak, ‘Lawful Access’; draft laws that died on the Parliamentary order paper; and finally a 2012 bill that had to be ignominiously withdrawn in the face of vociferous criticism from all sides, Canada remains exactly where it was more than a decade ago with regard to electronic surveillance powers. In the United States, there was controversy over the expanded surveillance powers in the *USA Patriot Act*. Then a few years later investigative journalism revealed that warrantless surveillance was being secretly practised by agencies regardless of the provisions of the law. In response, legislators (including then Senator and now President Barak Obama) hurried to simply rubberstamp the practice *post facto*. In the United Kingdom, where there was a longstanding threat of Irish Republican terror, the pre-9/11 *Regulation of Investigatory Powers Act 2000* provides wide scope for interception and enforced decryption of internet communication in the name of national security, not to speak of various other grounds.

Canada, under both Liberal and Conservative governments, has been a good and conscientious partner of its allies in fighting global terrorism, ready to do what seems to be required, even when this involves wrenching changes to long held Canadian values and ignoring international commitments to protect human rights. For instance, leaked memoranda indicate ministerial level approval of Canadian agencies under certain circumstances permitting the use of information from abroad that might have been gathered by torture and other ‘enhanced interrogation’ techniques that are abusive of internationally recognized standards. So why has Canada become an isolated outlier in relation to electronic surveillance powers? Are there any wider lessons to be drawn from this unusual position?
Some of the answer to the first question rests simply on circumstance. The passage of the Anti-terrorism Act was followed by four successive federal elections within a span of seven years. The first three of these resulted in minority Parliaments with the accompaniment of hyper-partisanship and persistent instability; the second in the defeat of the incumbent Liberals and their replacement by their Conservative rivals; only the fourth election in 2011 resulted in a majority Parliament. There have been three prime ministers over this span and even though the first two were Liberal, the transition between Jean Chrétien and Paul Martin was almost as fraught with political conflict as the later transition from Martin to Stephen Harper. In short, the political landscape was not conducive to easy passage of contentious new powers. Some legislative drafts simply vanished because governments were defeated or snap elections called.

The chaotic political context cannot entirely answer the question of why the dog never barked. A majority Liberal government was still comfortably in place when the Justice Department produced a ‘Lawful Access Consultation Document’ in 2002 that was submitted to separate rounds of consultation with public stakeholders (civil liberties and privacy advocates, etc.) and telecommunication industry representatives. This process, however, failed to produce a consensus. A second round of national consultation was carried out in 2005. Although any potential outcome of this second go-round was aborted by the defeat of the Liberal government in Parliament in late 2005 and the election of a Conservative minority in early 2006, it is unlikely that any basis for moving ahead had actually been achieved before the political upheaval. In any event, when long effort finally congealed in an actual legislative project before Parliament it was in the context of a stable majority government. The result was an embarrassing debacle and an ignominious retreat by the Tory government.

Some clues to this puzzle can be found in the public consultation rounds. I was a participant in these and can report that the civil society participants were generally sceptical if not downright hostile with regard to the civil liberties and privacy concerns generated by the Lawful Access proposals. Policing and security representatives were favourable but the consensus among civil society people was that the former had failed to make a coherent case for why new and enhanced powers were required, when old ones were still adequate. Obviously new technologies called for modernization and updating of legal language and in some cases perhaps for more extensive scope for warranted searches of data to match the new technological requirements. But the range of new powers being sought raised suspicions that government was seeking a fundamental expansion of its coercive reach into civil society using the pretext of the anti-terrorist panic following 9/11. There is, however, little or no evidence to suggest that this kind of criticism had made any impression on successive governments. To understand the hesitation in moving ahead we have to look elsewhere.

Parallel consultations with the telecom industry were held behind closed doors. There is evidence to indicate that the problem that emerged in this forum had little to do with privacy or civil liberties, but had much to do with the question of who would bear the costs of enhanced internet and telecommunication surveillance. There are two interconnected issues at play here. New technologies present a complex challenge to surveillance; state intervention will necessarily be expensive as counter-measures try to catch up, and keep up, with ever improving technologies. Prior to deregulation of the telecommunications sector, monopolies worked co-operatively in a spirit of public service to provide authorized information to appropriate law enforcement and security agencies; moreover, in an era before the explosion of new communication technologies, costs were relatively low and much of the burden was accepted by companies awarded a monopoly position in law. After deregulation and the emergence of a competitive and more technologically innovative market, telecoms became increasingly unwilling to bear the costs of more expensive surveillance measures. Well before 9/11, telecoms began to consider law enforcement and security services as simply customers rather than non-profit organizations carrying out public duties, and began shifting the costs of surveillance from the private to the public sector. Indeed, telecoms began building a profit margin into their dealings with police and security services even in the execution of court
orders. The Lawful Access proposals raised anxieties among the telecoms about how much of the cost of the contemplated new surveillance measures would be imposed on them.

Lacking consensus, especially in the crucial industry sector, successive governments simply put the Lawful Access project on the back burner where it easily fell victim to the shifting political vicissitudes of the latter part of the decade. Even though law enforcement and security services continued to pressure decision makers about the need to step up internet and telecommunication surveillance in the face of the continuing threat of terrorism and organized crime, not to speak of the need for Canada to keep up with its closest allies, public fears about terrorism were quickly receding as no attacks took place on Canadian soil (unlike Britain where the so-called 7/7 London Underground bombings greatly heightened anxiety levels). A minority Parliament in 2007 for instance ‘sunsetted’ the controversial powers of investigative hearings and preventive detention in the Anti-terrorism Act with no popular outcry. There was clearly no public pressure to force lawmakers to get on with a job promised in 2001 at a time of considerable societal alarm, but which now seemed to be losing its raison d’être.

With a Conservative majority government in place after the 2011 election, showcasing as one of its highest priorities a law and order agenda that included a tough-on-terrorism subtext, the stage seemed set for finally enacting a version of Lawful Access that might reflect some workable private sector-public sector consensus, even if civil society advocates remained skeptical. But when Bill C-30 landed in the House of Commons on Valentine’s Day 2012, pandemonium broke loose. The bill had been renamed, transformed from Lawful Access into something called the Protecting Children from Internet Predators Act. For ten years the primary target had been terrorist and organized crime networks. Controlling child pornography had been given at best some passing notice. Public Safety Minister Vic Toews revealed why the sudden change had been made when, weirdly echoing the notorious anti-terrorist maxim of George W. Bush, he told a startled and indignant opposition in the House that they were either ‘with us’ ‘or with the child pornographers.’ Mr Toews may have figured that this would intimidate opponents. Instead it poured gasoline on a fire.

It was the content of the bill that really ignited the blaze. Telecoms and internet service providers would be forced to install special surveillance devices to allow government access to a range of information on private usage. Where warrants are required, auditing and monitoring mechanisms are provided. Former Tory Public Safety minister Stockwell Day had promised to ensure that any new intrusive powers would only be exercised under warrants. But under C-30, governments could require without warrant the production of information on specified customers including name, address, telephone number and e-mail address, as well as the IP address and local service provider identifier. As one expert has pointed out, this would give police the capacity to scan the crowd at a demonstration to gather the identification of each cell phone and electronic device and then gather from the telecoms and ISPs the names and addresses of everyone so targeted. Since there is no persuasive evidence that police have been unable to gather the information they actually require for legitimate law enforcement purposes, this seems to many to represent disproportionate overreach.

The Tories badly miscalculated the political impact of C-30. They managed to stir up two very dangerous points of opposition. The internet community is one that governments around the world have learned to their chagrin not to mess with. Just a month or so earlier, a huge web campaign had forced the US Congress to back down on proposed legislative controls over the internet. Internet users are alert, technically savvy, and plugged into instant response networks. When governments or dot-coms like Google or Microsoft provoke this community, it reacts like a swarm of angry wasps. Vic Toews poked this nest and the wasps were all over him. A Twitter campaign heaped thousands of satirical tweets on the minister’s account informing him of the most mundane aspects of the tweeters’ lives—just in case he needed to know. Ontario’s Privacy Commissioner backed up the internet campaign by throwing cold water over the entire rationale for the bill and said it should be overhauled.
Perhaps more damaging to the government, C-30 set off a storm of opposition from the one area of Canadian society that matters most to the Conservative party, its own base. This was the same government that had killed the long-gun registry on the claim that it was a Big Brother state intrusion into people’s private affairs, and had killed the long-form census on the basis that the state had no right to demand details of people’s lives. Now it was offering a bill that seemed to give the state even more intrusive powers. Right-wing commentators attacked the bill; right-wing talk radio shows were buzzing with criticism; and even some backbench Tory MPs spoke out in an unprecedented show of independence in a normally disciplined caucus.

Faced with this barrage of criticism from across the political spectrum, Minister Toews and his government beat a hasty and humiliating retreat. For a time it seemed that a revised bill might reappear on the order paper, but that has yet to happen. Legislation restoring investigative hearings and preventive detention to the anti-terrorism arsenal has been introduced in the House of Commons, indicating that the Harper government has not abandoned draconian legal approaches to counter-terrorism. Yet despite public exhortations by the police chiefs and the Director of CSIS, there seems so far to be little enthusiasm for reviving Lawful Access under that or any other name. Some journalists have pronounced the project dead. Even if some version does arise again, it will surely be in a modified and tamed form given the depth and breadth of opposition the first instance inspired.

The surprising fact is that Canada finds itself in a unique position relative to its closest allies with regard to post-9/11 electronic surveillance in the name of national security. Is Canada’s position simply idiosyncratic, or are there any wider lessons to be drawn? We can reject culturist explanations, that Canada is unusually liberal compared to its neighbours: a glance at the policies of the current federal government on almost any issue should be enough to disabuse anyone of that notion. I would offer instead the following reflection. Assuming that Canadian political culture is not in fact widely different from that of its neighbours, the USA and UK, a set of fortuitous circumstances prevented the Canadian government from acting with the same haste as its allies in the face of an apprehended high threat level. As public perception of the terrorist threat has diminished, so has public acquiescence to greatly expanded state surveillance powers. Neither organized crime nor child pornography serve as substitute spectres to frighten the public into giving up more privacy and freedom of expression.

As the imminence of the terrorist menace recedes in both the USA and the UK, we may anticipate stronger resistance to any further demands for enhanced surveillance powers, or perhaps even growing insistence on rolling back some of the powers earlier usurped by the state. The internet community is an influential new actor on the world stage with global reach, capable of very swift and agile response to threats to its autonomy, access to information and freedom of expression. Healthy suspicion of state intervention in communication exists on all sides of the political spectrum. These slumbering giants of resistance were roused in Canada but they exist elsewhere as well.

By accident, despite itself, Canada has demonstrated a model of sorts for resistance movements in other countries.
Is there a future for online privacy?

Or, more pointedly, given that the vast capabilities of data analytics have come to be a lynchpin (if not the lynchpin) for much of government counter-terrorism activity, is there any way to square the need for counter-terrorism data surveillance with a sense of data privacy? In other words, can we have our cake and eat it too? Can we gain the national security benefits of dataveillance (to use a phrase that seems to describe the activity) while also protecting civil liberties and privacy?

It seems that the two will be increasingly in tension if we fail to adjust our conceptions of privacy to account for technological change. Just the other day, the European Network and Information Security Agency concluded that even if we wanted to create greater online privacy (through, in that instance, a right to be forgotten) the trend of technology is making that increasingly impossible to achieve—at least in the classic sense that privacy advocates mean, where a user is in complete control over data about himself.

For a number of years I have been writing critically about our current approach to this conundrum. I have none too charitably called the current set of privacy rules that form the bedrock of much of our thinking “antique privacy.” The more I see of the world around us, the more convinced I am that the description is apt.

Indeed, just after I sat down to begin writing this brief article, the Petraeus affair exploded into the American media (perhaps it made less of a splash elsewhere). While, obviously, the titillating aspects of the story drew the most attention, buried within the story was the, to me self-evident, realization that even America’s senior spy chief has little, if any, remaining digital online privacy.

What, then, are we to do about this? There is, I think, a better way. Let me outline it in this brief note.

First, if we are to adequately protect privacy we have to begin to recognize that privacy is an instrumental value, not, in my judgment, an absolute. By this, I mean that we need to look at privacy as a construct we use to protect other important values—things like autonomy, self-determination, democracy, and liberty of conscience.

In the context of national security dataveillance, the underlying value to protect is, I would posit, the value of anonymity—in effect, the ability to walk through the world unexamined. Or, perhaps more realistically, what we mean by anonymity is that even though one’s conduct is examined, routinely and regularly, both...
with and without one’s knowledge, nothing adverse should happen to you without good cause. In other words, the veil of anonymity that is now so readily pierced by technology must be protected by rules that limit when the piercing may happen as a means of protecting privacy and preventing governmental abuse. To put it more precisely, to my mind the key to reconceiving privacy in a way that effectively responds to the new technical reality lies with seeing privacy’s principal virtue as a limitation on consequence. If there are no unjustified consequences—that is, consequences that are the product of abuse, or error, or the application of an unwise policy—then, under this vision, there is no adverse effect on a cognizable liberty/privacy interest. In other words, if nobody is there to hear the tree, or identify the actor, it really does not make a sound.

All that is fine in theory, but what does it mean in practice? It seems to me that it means we must now focus a great deal more closely on the means/ends/consequence fit of any proposed dataveillance program. This idea of considering privacy in a retail way is, I think, fundamentally different from the wholesale, ex ante, way we think about privacy now. Under this paradigm, the questions to be asked of any dataveillance program begin with questions of its purpose, efficacy and scope: to what end is the dataveillance directed? How close is the fit between the data analytic questions asked and the end in question? Is it voluntary or mandatory?

Once we understand the means contemplated and the intended scope, we can ask a set of questions about the program’s effects on data subjects: what is the consequence of identification? What is the trigger for that consequence? Who decides when the trigger is met? etc. These questions are the ones that really matter, and questions of collection limitation or purpose limitation, for example, are, in my judgment, distractions from the main point. I don’t say this with joy, but rather in recognition of technological reality. Practitioners who maintain fealty to the existing privacy structures will, inevitably, find themselves in the backwater of policy making.

The right answers to these more particularized, retail questions of consequence will, of course, vary depending on the context of the inquiry. We will have a different evaluation of, say, a broad based airport screening program that uses link analysis to identify aviation security risk than we will of a more narrowly focused inquiry that, say, assists in the rendering of employment decisions in a critical industrial sector.

Perhaps you think this outline of retail consequential privacy analysis is still too theoretical. So to close out this short essay let me work through a few examples as a way of understanding some possible rule-sets for this type of analysis (all with the caution that my thoughts here are relatively tentative and subject to revision). Let’s consider four distinct situations where dataveillance might be applied:

1) Comprehensive data review as a condition of employment in a critical infrastructure (such as, say, a nuclear facility);

2) A similar review, but as a condition of employment in a non-critical sector (such as, say, education);

3) Voluntary data review as part of a frequent traveler program, like the Department of Homeland Security’s Global Entry/TSA Pre-Check program; and

4) Involuntary dataveillance of limited data set (name, DOB and gender) as a condition of airplane boarding, as with TSA’s Secure Flight program.

Our first cut at the analysis might look something like the below chart (where I am describing current practice, rather than an idealized vision):
<table>
<thead>
<tr>
<th></th>
<th>Nuclear Plant</th>
<th>Teacher</th>
<th>Global Entry</th>
<th>Secure Flight</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voluntary</td>
<td>No—unless you don’t want the job</td>
<td>No—unless you don’t want the job</td>
<td>Yes</td>
<td>Yes and No. You don’t have to fly—but if you choose to do so you must submit to Secure Flight</td>
</tr>
<tr>
<td>Goal of Dataveillance</td>
<td>Significant consequences (threats to critical infrastructure) with low probability</td>
<td>High probability but comparatively low consequence event (e.g. teacher molestation of a child)</td>
<td>High consequence (air hijacking or disaster) with low probability</td>
<td>—As adjacent—[Though note that early conceptions of the program included anti-crime goals as well]</td>
</tr>
<tr>
<td>Effectiveness/Fit</td>
<td>Tight fit—Narrow criteria and a focused threat.</td>
<td>Loose fit—Broader criteria and a broader threat</td>
<td>Medium fit—Broad threat with detailed screening</td>
<td>Loose fit—Broad threat with minimal criteria</td>
</tr>
<tr>
<td></td>
<td>Database sources likely include commercial</td>
<td>Also commercial sources</td>
<td>Exclusively government data sources</td>
<td>Also government data sources</td>
</tr>
<tr>
<td>Consequence of Identification</td>
<td>Loss of employment</td>
<td>Loss of employment</td>
<td>Secondary screening and/or denial of travel</td>
<td>Secondary screening and/or denial of travel</td>
</tr>
<tr>
<td>Trigger</td>
<td>Terrorist record or perhaps any criminal record</td>
<td>Criminal record or, more narrowly, child abuse record</td>
<td>Terrorist connection/watch list or criminal record</td>
<td>Terrorist connection/watch list</td>
</tr>
<tr>
<td>Standard of Proof</td>
<td>Negligible—Just a match</td>
<td>Negligible—Just a match</td>
<td>Detailed adjudication</td>
<td>Negligible—Just a match</td>
</tr>
<tr>
<td>Decision maker</td>
<td>Employer</td>
<td>Employer</td>
<td>DHS</td>
<td>TSA</td>
</tr>
</tbody>
</table>

So, what can we learn from this exercise? A great deal, I think.

For one thing, it strikes me as anomalous that the decisions that have the greater long-term consequence (e.g. denial of employment) are the ones that have the least significant degree of proof requirement and are adopted through the least formal decision making mechanisms. By contrast, the dataveillance program that is the object of the greatest public scorn (airplane flight screening) is the one where lesser consequences are imposed, fewer data sources consulted and a more formalized process of identification is used. We can speculate that this is because of the universal and involuntary nature of the program but, nonetheless, my preliminary thought (the most that can be offered in this brief note) is that much of our focus and concern for adverse privacy consequences may be misdirected at less significantly intrusive programs.

A second issue that leaps out from this discussion is that the standard of proof and the identity of the decision maker are all, at least for now, tied to non-judicial, administrative proceedings. We might well
consider whether or not there are certain dataveillance consequences that need a more formalized (perhaps *ex parte* judicial) approach.

I do not, in any way, suggest that the questions I have asked are necessarily the correct ones or that they are comprehensive. To the contrary, I suggest them as notional for the purposes of stimulating discussion and analysis. But to my mind they are the right questions to ask about digital privacy today. We would advance online data privacy far more if we reoriented our concerns away from worries about collection limitations and data retention rules toward a more robust understanding of consequential instrumentality.
Privacy rhetoric often focuses on the individual (Solove 2008). Computer systems are designed to give individuals control over their “personal” data while legal narratives often speak of individual harm and informed consent by individuals. Models that go beyond the individual often focus on groups (e.g., access-control lists that support bounded entities) or articulated lists of others (e.g., “joint rights” models that focus on multiple defined entities). But what are the implications of privacy in a networked world where boundaries aren’t so coherently defined and when entities aren’t so easily articulated?

Curious about what secrets might be hidden in my DNA, I decided to spit in a tube and turn my DNA over to the genetic testing service 23andMe. What came back was fascinating: hints that my ancestors might have origins that differ from the family narrative, and disease probabilities that suggest that family medical stories are either inaccurate or statistically curious. Through this test, I learned information about myself, but I also learned information about members of my family. Furthermore, by choosing to subject my DNA to this testing process, I didn’t just reveal data about myself; I gave away data that provides insights into my mother, brother, grandparents, and even children that I don’t yet have. I never asked my future grandchildren for permission to offer their data to a scientific database. I made a decision about the privacy of my data that affects numerous people who are implicated but who have no say. And, in doing so, I learned information about them that they may not wish to know, let alone have me know.

Our data—and with it, our privacy—is increasingly networked. What we share about ourselves tells heaps about other people. Sometimes, as with DNA data, we’re linked by immutable factors. In other situations, the connection is social or locational. I can’t even count the number of photos that were taken by strangers with me in the background at the Taj Mahal. And my friends often post photos of me with them without asking my permission. Yet, there’s also a third layer of connection. Our data also provides a probabilistic image of who we are based on comparisons to other people.

In the early days of personalization based on simplistic usage patterns, there were innumerable moments in which personal portraits were wrong in funny ways. Like many others, I had my “My TiVo thinks I’m gay” story. As an ethnographer who studies teen culture, I travel all over the United States where I grab Wi-Fi from truck stops and sleep in Motel 6s and hang out at too many fast food joints. A month into an intensive tour of the Midwest, I couldn’t help but notice that I was getting fascinating advertisements for grill guards, CB radios, and other accessories for my non-existent big rig. Google had pegged me for a long-haul trucker.

Machine learning algorithms have improved tremendously over the last decade and personalization has become so ubiquitous that most people are unaware of how their data is aggregated with others to
construct portraits of individuals that predict their interests based on others’ habits. Our interpreted selves aren’t simply the product of our own actions and tastes; they’re constructed by recognizing similar patterns across millions of people. How machines see us depends on how our data connects to others. The tastes and interests of people who don’t yet exist within systems can be easily predicted based on the patterns of others. And, when machines have access to a person’s social network, the predictions are even stronger. We aren’t as unique as those of us in the West might want to believe; we are the product of the people we know and the socio-cultural environment in which we are situated.

**Control and Interpretation**

Any model of privacy that focuses on the control of information will fail. Even achieving true control is nearly impossible because control presumes many things that are often untenable. Control assumes that people have agency, or the power to assert control within a particular situation. Control assumes that people have the knowledge and skills to truly control information. And control assumes that people understand the situation well enough to make informed decisions about what should be shared to whom and when. Furthermore, in a networked age, a reasonable amount of control is not enough; control has to be absolute control. One slip-up or data leakage and whatever was once protected can easily enter into a networked public where it may enter broader databases, be aggregated with other data, and circulate. In a networked world, data is more persistent, replicable, searchable, and scalable than ever before. Trying to achieve perfect control will only lead to frustration.

If we cannot rely on control to achieve privacy in a networked age, how then can we think about networked privacy? Focusing on articulated lists of relevant actors and trying to obtain rights from affected persons is bound to fail. There’s no way that consent from my not-yet-alive grandchildren is possible. This suggests that focusing on permission at the data acquisition level is not going to be viable. We need to understand privacy in context (Nissenbaum 2009).

Many of the teenagers I have interviewed have given up on controlling access to content (Marwick and boyd 2011). Nosy parents and friends who are “in their business” challenge their ability to have agency within social situations and, even when they think they understand the boundaries of a particular online social setting, they feel as though things change so fast that it becomes impossible to actually achieve control. Some try to achieve privacy through technical means or by simply demanding that adults “keep out,” but I’m fascinated by the diverse groups of teens who have taken a different tactic. Rather than trying to limit access to content, they work to limit access to meaning. They use pronouns and in-jokes, cultural references and implicit links to unmediated events to share encoded messages that are for all intents and purposes wholly inaccessible to outsiders. I call this practice “social steganography.” Only those who are in the know have the necessary information to look for and interpret the information provided.

Needless to say, even if teenagers’ efforts to achieve social privacy keep their parents in the dark, they don’t stop algorithmic interpretation—and misinterpretation—of their interactions. They are still subject to advertising and personalization based on what they post and they may be rejected by colleges and have limited job opportunities based on the interpretations of machines or people. But their efforts to achieve privacy without relying on the control of information are still an important signal. Not only have the next generation not given up on privacy, but they’re actually trying to find ways to achieve privacy in networked publics.

If we assume that the future of data is networked and that we can no longer rely on control of data to achieve privacy, it becomes imperative to look for alternate models for dealing with networked privacy. My guess is that we need to start by shifting to a model that focuses on usage and interpretation. Who has the ability—and the right—to interpret what data they think they see? In which domains is it acceptable to
discriminate based on interpretation of aggregate data? What are the mechanisms by which people can challenge how they’ve been interpreted?

**Looking Backwards, Moving Forward**

In Geoff Bowker and Leigh Star’s (1999) seminal text, “Sorting Things Out,” they detail the classification schemes used to describe people’s race under apartheid in South Africa. The population was divided into four racial categories—White, Black, Asian, and Colored—and their lives were configured accordingly. Housing, transport, and jobs were all segregated by race. But imagine what happens to families when a parent is categorized differently from a child or when siblings fall under different categories. Families cannot live together, kids aren’t able to go to school together, and parents cannot take their children to the doctor. Momentarily putting aside all of the injustices of apartheid, these categories become untenable as an organizational structure because people’s lives are interwoven with others’ lives.

The challenges of networked privacy are not new issues, but social media and networked culture magnifies them in significant ways. The data that underpins networked sociality and algorithmic life connects people across numerous axes time and time again. The future is only going to be more networked, more interwoven, more of a gnarly hairball that’s impossible to untangle without harsh cleaving. Expecting that people can assert individual control when their lives are so interconnected is farcical. Moreover, it reinforces the power of those who already have enough status and privilege to meaningfully assert control over their own networks.

In order to address networked privacy, we need to let go of our cultural fetishization with the individual as the unit of analysis. We need to develop models that position networks, groups, and communities at the center of our discussion. And we need to find a way to empower people by freeing them to share in ways that don’t negatively affect how others’ lives are interpreted.

**References**


In light of the hyperbole—and even hysteria in some circles—over an approaching privacy cliff and the informative and critical attention to privacy this journal has previously paid\textsuperscript{1} with respect to issues such as how privacy is light on being a social rather than only an individual value; how it can encourage an ad hoc, jerry-rigged technology-specific approach, rather than one grounded in a comprehensive theory of personality and human dignity; its tendency to slight questions of justice and fairness at the altar of individualism and property; and its tilt away from an equally important and terribly neglected question of publicity (with its obligations and rights to reveal, as well as protect information) (Marx 2011), we might be excused for bringing less than overflowing enthusiasm to yet another discussion of privacy. However, as Colin Bennett (2011) wisely notes, given our culture and popular understandings, it is likely the best term we have for public communication of the issues. That is certainly the case for online privacy with respect to consumer concerns—the topic we will discuss. Rather than dealing with the clouds of abstraction, strong advocacy of a normative position, or prognostication, we ask, “what are some of the findings of social science research for consumer’s online privacy concerns?”

Online commerce is big business and is expected to grow. In the U.S. in 2011, consumers spent about $200 billion online (www.internetretailer.com/trent/sales). A major factor that differentiates online from most offline conditions is the collection, retention, distribution, merging and use of personal information by online businesses and information brokers. Online companies claim that information collection allows them to personalize products and services to their customers and, by creating loyal customers, companies benefit (Culnan and Bies 2003). However, the benefits of personalization do not override privacy concerns for most consumers (Han and Maclaurin 2002). In fact, according to polling data, consumers have real privacy concerns about their personal information online (see www.truste.com/about-TRUSTe/press-room/news_truste_releases-us_customer_findings_report and www.webpronews.com/seriously-for-the-last-time-nobody-likes-being-tracked-online-2012-04 for 2012 polls). Unfortunately, too many online businesses fail to effectively address consumers’ privacy concerns (discussed below).

Privacy and trust are variables that predict online purchasing and purchasing intentions (e.g. Smith, Dinev and Xu 2011). However, privacy is an elusive concept (see e.g. Smith et al. 2011). Nevertheless, certain elements are common to a number of definitions: control over transactions between person(s) and other(s) and the goals of enhancing autonomy and/or minimizing vulnerability (Margulis 2003). Different interpretations of these elements and the inclusion of additional variables generate a variety of definitions of privacy, such as those found in many consumer online privacy studies. Common elements in definitions of trust are awareness of one’s vulnerability to harm by other(s) and a belief in the positive intentions of

\textsuperscript{1} e.g. the debate initiated by Colin Bennett (2011) in Surveillance & Society 8(4), http://www.surveillance-and-society.org/ojs/index.php/journal/article/downloadSuppFile/privacy_defence/privacy_debate
the other(s) toward one’s self (Fulmer and Gelfand 2012). A shared element, vulnerability, links privacy and trust. Vulnerability underlies consumers’ online privacy concern. Though studies agree that privacy and trust are related (e.g. Smith et al. 2011), there is no consensus on the nature of the relationship.

Although studies hypothesize that low privacy concerns and/or high trust in a website are antecedents of online behaviors, such as protective behaviors (e.g. Milne, Labrecque and Cromer 2009), relatively few studies have directly examined the influence of privacy and trust specifically on online purchasing decisions and intentions (see Smith et al. 2011 for a review). Most of those studies support that relationship (e.g. Milne and Boza 1999; Ranganathan 2012). However, the relationship is often influenced/moderated by additional factors, such as familiarity with an e-tailer (Van Slyke, Shim, Johnson and Jiang 2006).

Building trust is more effective (on average) than reducing privacy concerns for gaining competitive advantage (Milne and Boza 1999). Researchers have posed a number of ways to build trust. We address consumer trust and consumer privacy concerns by focusing on what Svenonius (2010) calls the “consumer rights regime”: the role of “legislation, consumer organizations and protection agencies, and mediation boards” on creating trust (2010: 313).

The U.S. Federal Trade Commission (FTC), a consumer protection agency, advocates five fair information practice principles (FIPPs) to address consumer privacy concerns. In brief, they are: notice of information practices; consumer choice on how personal information is used beyond its intended use; reasonable access to one’s personal information at a website and the ability to ensure its accuracy and completeness; the taking of reasonable steps to ensure the security of personal information at a website; and instituting an enforcement mechanism through self-regulation, enforceable regulations, or legislation (www.ftc.gov/reports/privacy3/fairinfo.shtm). The FTC has proposed a new privacy framework, based on best practices, that subsumes the five FIPPs and also addresses reasonable information collection limits, sound retention practices, and consumer education about commercial data privacy practices (FTC 2012).

Culnan and Bies (2003) argue that a company’s use of FIPPs addresses fairness by providing consumers with control and voice with regard to disclosures and by signaling that a firm can be trusted with disclosed information.2 If e-tailers were to fully implement FIPPs via privacy notices and supporting policies and procedures, consumers should have far fewer major privacy concerns. However, currently, the FTC’s FIPPs are not legally required because the FTC failed to get supporting legislation for this policy.3 To extend its legal reach, because many companies, online and offline, have failed to effectively implement the five FIPPs (see below), the FTC again has called for supporting legislation to put legal bite in its new framework.

However, from Congress’ perspective, self-regulation by online firms, if it was consumer responsive, would probably make legislation unnecessary (Culnan and Bies 2003). But just how effective online self-regulation has been for consumers is an open question. Several studies report that most companies’ privacy policies do not include all the FIPPs (e.g. Sheehan 2005). Moreover, many privacy policies are not understandable (Culnan and Bies 2003). Their purpose is too often to reduce the company’s liability, not to protect the consumer (e.g. Papacharissi and Fernback 2005). Although consumers prefer websites with privacy notices over those without them (Pan and Zinkhan 2006), only about 30 per cent of consumers closely read a website’s privacy policies (Consumer Awareness Project 2009 at www.cdt.org/privacy/guide/surveyinfo.php; also see Milne and Culnan 2004). We are left to wonder whether the FTC’s new framework will be any more successful than its five FIPPS if it lacks legislative support.

---

2 Currently, there is no consensus on the nature of the relationship between fairness and trust.
3 Only if a firm’s business practices are deceptive or fraudulent can the FTC can take legal steps.
Moreover, because the U.S. views privacy as a relative, not an absolute, right, Congress has resisted general consumer privacy legislation in favor of limited sectoral legislation, e.g. protection for children online and of video rental, medical and financial records (see e.g. Langenderfer and Miyazaki 2009). For example, three general privacy bills, and a fourth aimed at children and teens, plus eight bills addressing data security and data breach notification (FTC 2012: notes 16, 18 and 19) have languished in the current (112th) Congress. One explanation of Congressional resistance is that such legislation has the potential to increase the cost of conducting business, hence lowering profits—a particular concern to low-margin companies (Smith et al. 2011). Regan (1995) provides another explanation. Framing privacy as an individual right (interest) has had a weak impact on congressional policy-making because it enables groups that would bear the costs of the proposed privacy legislation to eventually shape or undermine the privacy legislation by asking that individual privacy interests be balanced with presumably higher interests that serve the public good, such as organizational efficiency and business competitiveness. In this regard, polls on privacy concerns seem to focus on privacy as an individual good, not a public good. That most consumers have moderate, not high, privacy concerns (Sheehan 2002) is potentially another basis for resisting legislation. If consumer privacy legislation is to be enacted, Culnan and Bies (2003) argue what we should expect is sectoral legislation, a convergence of business and consumer interests, and strong media attention to the issue. Might opinion polls on consumers’ privacy concerns stimulate legislation? That’s uncertain. Gandy (2003) argues that because private corporations are the primary sponsors of privacy polls, these polls and their authors have nudged the policy debate toward self-regulation as the answer. All of these factors work against Congress passing strong consumer privacy legislation.

There are some organizational bases for increasing trust and reducing privacy concerns. One example is the third-party guarantor, such as TRUSTe. TRUSTe provides its clients—commercial websites—with a privacy seal of approval “suited to [its] business practices” and compliant with “federal and state requirements” (www.truste.com). Operationally, the seal addresses two FIPPs: notice and choice. (www.truste.com). Privacy seals are associated with greater trust in a website and a more favorable attitude toward the company’s privacy policies (see e.g. Miyazaki and Krishnamurthy 2002). Also, a commercial website’s reputation can increase a consumer’s trust in a website (see Li 2011 for a review). In this regard, some websites provide reputational indicators of vendor trustworthiness, such as eBay (using consumer feedback on online sellers) and Angie’s List (using consumer feedback on offline service providers).

TRUSTe reports that its seals positively impact consumer purchasing. Unfortunately, other studies report that a privacy seal does not necessarily mean better privacy practices or the collection of less personal information (see Smith et al. 2011 for a review). Moreover, a study of online advertising found that only those consumers who had both prior negative attitudes toward advertising and a high desire for privacy had more positive purchase intentions because of privacy seals (Stanaland, Lwin and Miyazaki 2011). Finally, a privacy seal is no guarantee that a website is free of malware or spam. One study found a higher rate of malware and/or spam at websites with a TRUSTe privacy seal than those without it (www.benedelman.org/news/092506-1.html).

In the absence of legislative or regulatory or reputational protection, a potential protection for a consumer with a grievance against an e-tailer is alternative dispute resolution (ADR), the threat of which might deter bad practices or at least offer some redress to those wrongly treated. The most common form employed by offline companies is binding arbitration. Among its disadvantages to consumers is its potential to be expensive and that the vendor might choose an arbitrator who has favored the vendor in the past. (http://www.nolo.com/legal-encyclopedia/arbitration-clauses-contracts-32644.html). By comparison, mediation is common in Europe (Svenonius 2010). In this regard, TRUSTe will mediate online, eligible

---

4 There is also a threat posed by websites that “copy and paste” a legitimate privacy seal onto their own website, presumably a deceptive practice that the FTC could investigate.
privacy complaints of consumers against client websites without cost to the consumer. TRUSTe’s determination is not legally binding on the consumer (unlike binding arbitration) but it is binding on the website. Moreover, consumers can appeal decisions and TRUSTe punishes uncooperative websites (http://www.truste.com/products-and-services/dispute-resolution-services/dispute-resolution-faq). What is needed is research on websites’ use of ADR: its forms, their frequency, and consumers’ judgments of ADR’s efficacy, trustworthiness, and fairness.

Another potential contribution to addressing consumer concerns involves Privacy Impact Assessments (PIA). Wright and de Hert (2012) and colleagues from several disciplines have critically analyzed this emerging privacy tool. The policy tries to anticipate problems, seeking to prevent, rather than to put out, fires. The PIA model is adopted before personal data practices are established. It involves a variety of stakeholders and tries to learn from the past and to imagine how new technologies and practices might bring new problems—including that intriguing class of the “unknown unknowns.” Marx (2012) offers a critical analysis of the tool and calls for conceptual elaboration with respect to the kinds of privacy problems that appear and the stage of the surveillance process or cycle where they appear. PIA is very much a work in development but offers a model for raising awareness and for trying to bring some balance to conflicting interests. On the other hand the practice is voluntary. Thus, in the final analysis, and consistent with American political economy, we conclude caveat emptor.

References

*Surveillance & Society* 10(3/4) 354


1. Where Are We?

When trying to establish whether privacy is dead or whether it is merely evolving, we may very well be asking the wrong question. While there is considerable evidence that the concept of privacy is undergoing a sea change in the eyes of both individuals and policy makers, it could be argued that this is merely an expression of a much more fundamental issue that underpins the technological, political and economic changes we have witnessed over the past decade.

It is true that anecdotal evidence suggests that individuals, both as citizens and consumers, no longer value their privacy the way they once did. Many claim that this is true in particular for younger people who seem increasingly comfortable with sharing even intimate details about themselves and their life with others, including a much wider range of “others” than their parents’ generation would have done.¹ Much of this is attributed to the evolution of the “participatory culture” (Jenkins et al. 2006) that has developed online and that has shifted social interaction, as well as the expression of one’s creativity to mediated spaces that allow for maximum interaction, but that also require a much higher level of individual exposure not only to the other participants in those spaces but to the intermediary.

Nevertheless, successive studies have shown that the wish for control over one’s own information remains high with, for example, 78 per cent of respondents to a 2011 EU survey on privacy believing that their specific approval should be required before any kind of information about them is collected and processed (Eurobarometer 359, 2011). While awareness of potential intrusions may be lower than it once was (possibly due to the way in which many online services manage to create an atmosphere of selectiveness and intimacy where in practice there is none), it is increasingly clear that a general feeling of unease over unauthorized access to personal information prevails and that a sense of encroachment in cases where contextual boundaries of information control are breached remains (Nissenbaum 2010). Thus, teenagers who are happy to share with their peers details of their daily experiences, thoughts, emotions and social interactions will often go to extraordinary length to prevent their parents, teachers or others in authority over them from accessing those spaces they consider to be private (boyd and Marwick 2011). Similarly, the outrage at perceived violations of those spaces is real, as is the lack of trust that results from experiences of repeated intrusions and the unexpected shifting of boundaries, in particular by those providing those spaces or those who provide access to them.² In the EU, almost two thirds of consumers do not trust their telephone, mobile or internet access providers or providers of online services (search,
social networking, etc.) to protect their personal information. In historically privacy-conscious Germany, the numbers are even higher (between 74 and 78 per cent) (Eurobarometer 359, 2011).

The reason why those consumers continue to provide their personal information to providers they do not seem to trust can arguably be found in the realization that, in order to be part of this new participatory culture, the disclosure of personal data has become inevitable, a take-it-or-leave-it offer on the part of providers who turn personal data into a new currency used to pay for many of the “free services” they offer (Eurobarometer 359, 2011). This approach sets people’s desire to protect their personal information against their materialistic and social wants and thus effectively re-defines personal data as a freely tradable commodity.

At policy level, individuals’ apparent acceptance of this commercial privacy trade-off has enabled a line of argument to develop that claims that no new regulation of personal data processing is required (and that, indeed, the existing rules should be relaxed) precisely because there is no obvious demand for such regulation (Johnson 2010 and Spiegel Online 2012). In the ongoing conflict between the individual’s right to privacy and the commercial need for the free flow of personal data as an ever more important resource in the modern information society, this increasingly results in an emphasis of the economic importance of personal information, which is classified not merely as a business interest but as a common societal good (Reding 2012). At a time of global recession, the economic imperative has therefore joined “national security” as the public policy objective of choice to which individuals’ privacy is expected to take a backseat.

However, this view ignores the possibility that much of consumer inertia in this area could be attributed to a general sense of powerlessness within populations where individuals, particularly in the online environment, uncritically accept privacy statements that authorize wide-ranging uses of personal information, often without reading them, not because they are not concerned about their data but because they know that, in reality, their choice is between accessing online services on the providers’ terms or not at all (Edwards and Brown 2009). The transparency approach, originally designed to provide consumers with agency in their dealings with commercial partners, could therefore be said to have spectacularly failed to enable consumers to maintain any kind of control over their personal information that would still allow them equal participation in social and economic life in the 21st century.

More importantly, however, proponents of a more relaxed regulatory approach to the protection of personal data also wilfully ignore the traditional historical objectives for establishing a right to privacy, particularly within the continental European fundamental rights tradition. This tradition has never viewed privacy merely as an individual right, but as a societal or common value that must be upheld in order to protect “democratic substance” (Simitis 1984). Within this paradigm, there is no clear binary conflict between the right to privacy on the one hand and economic or security interests on the other. Rather, it views privacy as an essential instrument designed to assist in maintaining the delicate balance of power between individuals, commercial entities and public bodies that our democratic constitutional systems were set up to create and uphold. A need for privacy will therefore not solely show up in the “consumer” column of the societal ledger, but also in that column which includes the measures that protect the constitutional structure. A shift of power in one direction or the other is likely ultimately to not only affect individuals’ (commercial) rights and freedoms, but also the foundations of democratic government itself. This has never been more clearly recognized than in the 1984 Census decision of the German Constitutional Court in which it accorded German citizens a right to informational self-determination (German Constitutional Court 1984). This right guarantees those citizens’ ability to retire to an unobserved private sphere where they can process information and develop ideas and opinions without being subjected to undue influence by public or private entities that may, in other spaces, have power over them. It was therefore seen as an essential pre-requisite for the active participation of the citizenry in political life.
Viewed in this way, it is easy to see that contemporary arguments which advocate a concept of privacy as a more proprietary right, and which bestow on individuals the power to freely trade (or not) in their personal information, largely and purposefully ignore the much wider objective that historically informed the fundamental right to privacy and data protection.

2. What should the future look like?

With this in mind, the question arises whether we can really limit regulatory interventions to those that are mandated by “the reasonable expectation of privacy” of the average consumer. All too often this approach seems to weigh the balance in favour of the interests of commercial providers and law enforcement agencies, who will inevitably proceed to engage privacy advocates in lengthy and often fruitless discussions about what is “reasonable” in a given situation. As a general rule these discussions do little more than distract from the underlying tensions that must be resolved (the recent discussion that surrounds the new DNT standard is a point in case here), while adding almost nothing to the development of an appropriate privacy standard.

Instead of engaging in these discussions, stakeholders should seek to answer some of the more basic questions that underpin the fundamental rights edifice, namely, what kind of society do we want to live in and what kind of sacrifices (economic, political and technical) are we prepared to make for establishing that society?

To fulfil the right to privacy’s original intention and promise would require us to take account not only of the short-term costs and benefits of an open exchange of personal information, but also the long-term risks we may encounter and the harms we may suffer—both as individuals and as citizens—if we continue to apply a relatively undiluted caveat emptor principle with regard to the collection and use of our personal information. A shift in emphasis from an instant gratification society to one that properly assesses and addresses long-term risk on the basis of ethical considerations is likely needed, not only with regard to environmental and climate concerns and economical and financial management, but also in the area of information rights. From Big Oil and Big Money to Big Data, the underlying questions remain the same, as do the political power structures within which those questions must be addressed.

Substantively, this may mean that privacy rights must be afforded greater weight when being balanced against competing interests, including economic and national security interests. In particular, we need to stress and acknowledge that those interests are not binaries in a zero sum game, but that instead an increase in privacy can result in increased economic success and improved security. Economically speaking, privacy-friendly business models, particularly online, may help establish and maintain users’ trust in online services, which they may otherwise choose not to use in order to protect themselves. In the future, this is likely to be increasingly important particularly for those types of services that rely on being able to process large amounts of personal data (for example, social networking services and cloud computing services). Although social networking services have seen exponential increases in their user base since their inception, that growth has recently slowed as those services’ ever more permissive approach to their users’ privacy has hit the headlines.

As already explained above, in terms of national security it could be argued that this should be viewed in a wider sense than merely the defence of a nation against an external or internal enemy. In a democratic state based on the rule of law, attention should also be paid to any threat that is posed to a nation’s wellbeing through the corruption of its constitutional institutions and tenets. Shifts in the balance of power between those institutions, business and citizens, which may easily arise from an “information imbalance”, where one actor is able to exercise control over another based at least partly on what they know about them, are likely to reverberate throughout society, possibly to the point where the original constitutional settlement is put at risk. Protecting its citizens’ right to privacy is likely to go some way...
towards ensuring an appropriate “information balance” and thus those citizens’ continued participation in the defence of those tenets and institutions. A lack of privacy protection, on the other hand, is likely to facilitate a division of society into privacy haves and have-nots, resulting in the likely disengagement of at least part of the population from the democratic process. A stronger global consensus on the need for enhanced privacy protection is therefore imperative, as a “race to the bottom” in which each country argues for a further watering down of privacy standards, ostensibly in order to provide its business community with a short-term competitive advantage (in this context, parallels may again be drawn between the data protection and financial and environmental regulation), risks much greater harm further down the line.

3. And what is the best means of acquiring that future?

In order to achieve this aim, we will have to ensure that the existing defensive discourse around data protection is replaced with a positive agenda for privacy. In the words of Nigel Shadbolt, Professor of Computer Science at the University of Southampton, we need a Warnock-style enquiry into the moral, not just the legal, framework that should govern our use of personal information (Rooney 2012). The Warnock Commission, which was established in the UK in 1984, inquired into the societal risks and benefits of human fertilisation and embryology. In the introduction to its report, the Commission describes its task as examining the “ethical implications of new developments in the field” directing its attention not just “to future practice and possible legislation, but to the principles on which such practices and such legislation would rest” (Department of Health and Social Security 1984). We are now at a point where we need a similar ethical enquiry into the kind of personal data processing that we, as a society, believe should be permitted, including types of data to be used, and the purposes for which they should be processed. Within such a context, we must distinguish clearly between those processing activities that are both individually and socially useful and those that are likely to pose a long-term threat to our societies.

Countries where strong privacy protection exists (like most of the EU member states) should resist external pressures to relax their regulatory requirements, and transfers of data to countries without appropriate privacy standards should be restricted much in the same way, as is the case under the current EU data protection framework, until binding international standards based on such an ethical enquiry can be agreed.

To prevent any use or exploitation of personal data that is not authorized by the individual to whom it relates, or that is not otherwise justified by internationally agreed public policy objectives, increased emphasis should be placed on strategies to achieve data minimization. This would most likely require a change in the mind-set of many designers and developers from an unfettered open data approach to a more socially responsible culture of innovation. While the former makes almost no distinction between the processing of personal and other information, thus viewing a technology’s use of personal data as a non-issue at best and as a value-added service at worst, the latter understands privacy features in terms of an application’s functionality rather than its limitations. Under the latter approach, a data minimization requirement would therefore be viewed as a design challenge rather than a barrier to innovation. While it would be preferable for developers to embrace this approach willingly for the reasons set out above, the current commercial focus on the large-scale exploitation of personal information may make a legislative mandate along the lines of some of the new principles included in the proposed reform package for a new EU data protection regime3 unavoidable.

Special attention should also be paid to the development of social norms regarding privacy in the online environment. In particular, greater emphasis should be placed on promoting an increased awareness of

---

3 For example, the obligations on EU data controllers to ensure data protection by design and by default (Article 23, draft Data Protection Directive) and data portability (Article 18, Draft Data Protection Regulation).
information rights and obligations from early-years education for children (see, for example, Ewart and Tisdall 2012) to lifelong learning projects for so called “silver surfers”. In considering our own moral framework at a very personal level, the question all of us should be encouraged to ask ourselves when processing our and others’ personal information is not, “what do I want to do?”, “what am I able to do?”, or “what am I allowed to do?” but “what should (and shouldn’t) I do?”

On a legal level, countries should consider adopting a consumer protection-style legal framework that moves away from the caveat emptor approach to the trade in personal information referred to above. Without restricting the individual’s personal autonomy and their general right to share their personal information with others, the limitations of the current transparency approach should be acknowledged by placing legislative constraints on the processing activities to which individuals may lawfully consent and on the “other” legal grounds on which those processing activities may be justified. Mirroring established principles in consumer protection law, privacy statements that seek to authorize legally restricted processing activities should be capable of being declared void or voidable.

Finally and most importantly, public bodies should pay renewed attention to the overarching policy objectives that have always underpinned the fundamental right to privacy and data protection. Where those objectives override or are even necessary to support other objectives like administrative efficiency, national economic interests or national and public security, a self-denying ordinance should be imposed that prevents the unfettered access by public bodies to data held by other public bodies or by private entities or that at least limits such access to that which is absolutely necessary and proportionate. Measures to support such an approach would include much stronger constitutional restrictions on data use and data sharing, the strict imposition of a burden of proof on public bodies that access to and further processing of such data is necessary (rather than merely useful), as well as strict procedural requirements for obtaining such access in the form of warrants or court orders.

Given the current lobbying assault by large multi-national data controllers on the European Commission in the context of the review of the EU data protection regime, it is difficult to believe that the political will to carry out a root and branch examination of the need for a right to privacy is there. However, politicians and policy makers that now shy away from this difficult task may wish to review their position in light of the experiences made in recent years with regard to the global approach to a relaxing of the rules for the regulation of financial institutions. Short-termism, while generally politically expedient, will almost always result in increased long-term risk and expense. The question is whether a loss of information privacy is a cost our societies can afford to bear.

References

Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (draft Data Protection Regulation), COM (2012) 11 final, Brussels, 25.1.2012


German Constitutional Court. 1984. “Census” decision (in German), BverfGE 65, 1

Jenkins, Henry, Katie Clinton, Ravi Purushothma, Alice Robison and Margaret Weigel. 2006. Confronting the Challenges of Participatory Culture: Media Education For the 21st Century. Chicago: The MacArthur Foundation


