Surveillance & Society

Debate | Talkin' About A Revolution

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 nation-wide 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

Vonn, M. 2012. Talkin' About A Revolution. *Surveillance & Society* 10(3/4): 336-339.
http://www.surveillance-and-society.org | ISSN: 1477-7487

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 tradescraft' 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 ramification 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

Nedelsky, J. 1990. Law, Boundaries, and the Bounded Self. *Representations* 30: 162-89.