Special English Edition 2012/2013 Annual Selection of Articles

editorial
Novática: Reaching beyond International Borders
> 02
Didac López Viñas, President of ATI

From the Chief Editor’s Pen
Privacy: Our Contribution to a High-Level Debate in the Digital Age
Llorenç Pagès Casas, Chief Editor of Novática

monograph
Privacy and New Technologies
Guest Editors: Gemma Gal handy Clavell and Gus Hosein

Presentation. Privacy, Technology and Policy: Social Networks, Data Mining and Surveillance
Gemma Gal handy Clavell, Gus Hosein

Privacy and Surveillance Primer
Aaron Martin

European Data Protection and the Haunting Presence of Privacy
Glòria González Fuster, Rocco Bellanova

Secrecy Trumps Location: A Short Paper on Establishing the Gravity of Privacy Interferences Posed by Detection Technologies
Mathias Vermeulen

Surveillance Technology and Territorial Controls: Governance and the ‘Lite Touch’ of Privacy
Darren Palmer, Ian Warren

Google: Navigating Security, Rights to Information and Privacy
Cristina Blasi Casagran, Eduard Blasi Casagran

Human Traces on the Internet: Privacy and Online Tracking in Popular Websites in Brazil
Fernanda Glória Bruno, Liliane da Costa Nascimento, Rodrigo José Firmino, Marta M. Kanashiro, Rafael Evangelista

Social Networks and the Protection of Personal Information. When Privacy Is Not Perceived As a Right
Massimo Ragneda

Privacy and Body Scanners at EU Airports
Joan Figueras Tugas
Privacy and New Technologies monograph

Privacy and Surveillance Primer

1. Introduction

In business and technology circles it’s in vogue to declare the death of privacy. Mark Zuckerberg proclaimed it. So did Eric Schmidt. The incredible popularity of social networking sites, free apps, and online services bears testament to the vast changes taking place. Even simple words like “free” don’t mean what they once did. Using a free platform is supposedly now equivalent to giving consent for personal information to be collected, manipulated, and sold. “If you aren’t paying for it, you’re the product,” or so they say. In this new, wondrous digital economy, personal data is hard currency. The platforms have become such an integral part of society that coughing up a name, an e-mail address or some browser history seems a small price to pay in exchange for access to the mainstream. This is exactly the kind of voluntary disclosure Zuckerberg talks about, but it isn’t always voluntary and it definitely isn’t “free” in the traditional political sense of the term.

The reality is, of course, much more complicated. The arguments that Zuckerberg and others make are naively perhaps intentionally naive. Privacy isn’t dead and it will likely never die, even as new data-intensive business models proliferate and surveillance becomes less expensive, more effective, and far more pervasive. Who governs and makes use of personal information is what’s most at stake: Facebook wants to govern rules for sharing, but more importantly wants dominion over vast amounts of information about what we do and who we know; Google competes to know more about what we’re seeking and do and who we know; and surveillance landscape.

2. Privacy as a Problematic

Privacy is one of society’s most contentious concepts. Scholars love to quibble about the definition of the term. There’s some debate as to whether privacy is an exclusively Western construct that makes little or no sense elsewhere. Culturally relativistic arguments apply equally to many issues, but the appeal to cultural relativism is also one of power and opportunity; we rarely entertain debates about copyright being culturally relative. Different cultures may define what’s private in dissimilar ways. Often the problem is finding the appropriate language to discuss privacy-related matters with those of a different culture, society or community.

Communitarians such as Amitai Etzioni argue that privacy rights must be balanced with the common good that individual privacy rights cannot be absolute [1]. Proponents of communitarianism offer a set of criteria for balancing the right of the individual against the good of society, including assessing privacy-friendly alternatives, aiming for minimal intrusion into one’s private life, and reducing undesirable side-effects. These principles are reflected in many international statements on privacy and human rights.

The modern challenge is to consider how these debates are reflected in our technological societies and changing economies. Sure, privacy must be balanced and the criterion may differ across legal systems but how is this negotiated when we consider the design of new technological infrastructures? Do we install the ‘balance’ into our designs, perhaps by ensuring that all computers have backdoor vulnerabilities for police to gain access? Similarly, technology is changing the modern family environment and there are new challenges about privacy that we must consider with regards to relationships and children. But protections could be democratized by only be available to the dominant forces within societies.

3. Framing the Debate

While these critiques are important and force us to think critically about the value of privacy, none of them offers a total rebuttal [3]. An essential systematic treatment of the concept comes from the legal scholar Daniel Solove, who provides some practical clarity in his *Taxonomy of Privacy* [4]. The taxonomy captures the various facets of privacy without dismembering or disinforming it. Solove moves past theoretical disputes (is privacy a human right, legal right, consumer right, cultural construct, etc.?) to explore more practical evidence of privacy in action: *activities* that pose privacy problems. He identifies four main categories (collection, processing, dissemination, and invasion) unpacking each...
Much has been said about ICT’s democratizing capacity. Yet less remarked upon is how the Internet and related technologies democratize surveillance as well.

in depth, and providing a solid framework to organize debate on privacy and surveillance.

This debate is everything. If privacy is a negotiated right, one that must be balanced against other rights and for national security, or for economic progress, we must have a debate about how the lines are drawn. The lack of debate is what leads to the greatest incursions. The inability to revisit older debates may be an inhibitor to progress and innovation. Therefore the promising aspect about privacy is that in many key places the debate is ongoing, and getting louder and stronger. That, if anything, is a good thing.

4. Processes of Surveillance: Categorization and Social Sorting

Privacy isn’t just an individual condition. On a macro scale, sociologists of surveillance such as Oscar Gandy [5] and David Lyon [6] have illuminated different ways in which information technology operates to discriminate between people and groups of people, for the purpose of controlling them.

Surveillance is a layered process. Before surveillance comes categorization, which is actually a two-step event: label first, then classify. We do this all the time; male and female, credit-worthy and sub-prime, ‘safe’ traveler and potential threat, etc.

There’s nothing inherently bad about categorization. As Michel Foucault made clear in *The Birth of the Clinic* [7], categorization is a key component of human knowledge and an indispensable aspect of our power to change our reality. First we distinguish between ‘healthy’ and ‘sick’, with obvious practical benefits. Then we distinguish between people with eye problems and people with foot problems, for example, and so it goes down the line. By grouping together like patients and removing outliers, we learn more about their condition and through that knowledge we gain the power to change it. Of course, categorization has its dark side too. Someone branded ‘criminal’, is associated with other criminals, and may continue to be associated with that group even if officially exonerated.

Categorization is important because it facilitates social sorting. Once subjects are labeled and bundled, they can be sorted, managed, and potentially controlled, which could have the beneficial impacts Foucault observed in the clinic but could also degrade fundamental rights and freedoms like movement and speech, and even life chances. Scholars concern themselves with the detrimental aspects of surveillance, but deserved scrutiny shouldn’t negate the potential upside. This isn’t about a trade-off; it’s simply to say that when these practices aren’t transparent or go unquestioned, the potential for negative outcomes increases. Privacy advocates continually expose and dissect systems of surveillance and categorization to understand their logics, operations, and social consequences to find the border between their beneficial and deleterious applications.

5. Sites of Surveillance

Mapping this border is more like mapping galaxies than distinguishing between rooms in a house: knowing where to look is a precondition of both, but a much more severe challenge in the first instance than the latter. Consequently, discovering where surveillance happens is becoming increasingly important. There’s a long and growing list of sites of surveillance, regularly padded by advancements in technology and new policies that require increased information collection.

Many of these sites, like airport security checkpoints, are familiar and normal to us, though the underlying politics involved is less clear, as Mark Salter’s work shows [8].

Some sites are less obvious. Our bodies are regularly sites of surveillance, as biometric devices and body-scanners work to categorize us based on our physical characteristics. Workplace surveillance is also a commonplace (e.g., monitoring of Internet activity) and schools are increasingly sites for surveillance (through video recording, electronic attendance tracking, etc.), as Torin Monahan and colleagues have shown [9].

Surveillance in public places is becoming the norm in our cities, especially as the technology to monitor these spaces gets cheaper and easier to use. During protests and large gatherings public surveillance is often intensified for crowd control and law enforcement purposes, such as during the Occupy Movements. Identifying the difference between public and private spaces and the corresponding rights to individuals has long been controversial, but new borders in our lives and the new spaces we create give rise to new rules and domains.

Despite its prevalence, surveillance isn’t equally distributed throughout society. Some groups are easier to monitor than others. For example, John Gilliom has documented how the poor (he studied low-income Appalachian mothers) are disproportionately subject to state monitoring [10]. We can all appreciate the state’s public duty to prevent benefit fraud and other undesirable actions, but we cannot lose sight of the potential for economic and political disenfranchisement that can result from heightened surveillance. We must therefore critically examine how the sites of surveillance are distributed to see how this affects the potential for an open and equitable society.

Online monitoring (or ‘cyber-surveillance’) provides an interesting twist to the idea of ‘spaces’ for surveillance. The extent to which cyber-space is actually a space is debatable [11], but the fact remains that surveillance is rampant online.

Both the Internet and mobile phone networks lend themselves to extensive information collection and tracking. Online surveillance was primarily commercial for many years, driven mostly by the desire to restrict access to content based on user location, and to deliver advertising. Recently however, political surveillance has intensified online, with the Arab Spring being a recen and powerful example. Dissident activities were organized online and threatened governments tried desperately to identify dissidents.

Cyber-surveillance also alters the socio-economic dynamics of privacy. Gilliom’s welfare recipients were disproportionally watched by state agencies but the economies of scale for surveillance online and over mobile phone networks make it very easy to identify, categorize, and discriminate everyone that’s connected. Much has been said about ICT’s democratizing capacity. Yet less remarked upon is how the Internet and related technologies democratize surveillance as well.

6. Modes of Surveillance

The how of surveillance is likewise complex. These are the various modes of surveillance.

When asked about surveillance, most of us think of visual monitoring. Orwell’s Big Brother in 1984 was always watching, and that association has stuck. While visual monitoring is no doubt an important form of surveillance, it isn’t the only one we ought to be concerned about.

Now what’s observable need not be visual. ‘Dataveillance’ is a rising challenge. Roger
Biometrics automatically identify or verify people based on features of their bodies. The technologies and techniques for biometrics include facial recognition, iris scanning, digital fingerprinting, and DNA profiling, to name a few.

In *Our Biometric Future*, Kelly Gates explains why facial recognition technologies were deemed a solution to the problem of international terrorism following 9/11, and explores what had to be neglected or glossed over about the technology for it to be seen as an appropriate security solution to the complex and multi-faceted challenges of combating terrorism [16]. The commonly held belief that our true identities are contained in our bodies means that this form of surveillance is likely to continue expanding.

Common beliefs aside, it is simple fact that none of these modes offers perfect information about a person. Each only permits a partial and limited understanding of our identities, relationships, whereabouts, communications, and so forth, depending on what information is collected and how accurately it may be in the form in which it’s obtained. Still, the organizations and industries driving new surveillance innovations strive to reduce these limitations, with the ultimate (but impossible) aim of achieving perfect, ubiquitous, all-knowing surveillance.

7. Subjectivities of Surveillance

Nonetheless, surveillance doesn’t need to be perfect to be effective. Even imperfect surveillance can be a tool of social control because it tends to result in self-censorship and behavioral inhibition. This is one of the most important ideas on surveillance, first intimated by Jeremy Bentham and later developed by Foucault.

Bentham’s Panopticon was a prison designed such that a guard could watch over all the inmates without them knowing whether or not they’re being watched (see Figure 1). The mere possibility of being watched was thought to be sufficient to condition good behavior.

In the Panopticon, it isn’t that those with nothing to hide have nothing to fear, but rather that the prisoners have everything to fear because they have no way to hide. Therefore, they regulate their behavior on their own, creating a normalized society without physical coercion. In *Discipline and Punish: The Birth of the Prison*, Foucault expanded Bentham’s principal to all of society, which he thought disciplinary by nature. For Foucault, it isn’t just prisons that normalize our behavior, but nearly all institutions [17]. The mere possibility of being watched is thus enough to modify behavior. As dissident Libyan journalist, Khaled Mehiri, remarked following the fall of Gaddafi: "Surveillance alone is enough to terrorize people" [18].

8. Political Economies of Surveillance

Again and again, we’ve seen private companies pop up as key drivers of innovations in surveillance and privacy. The political economies of surveillance are thus worthy of examination. Which business models require the extensive collection of personal information and how do these business models regard privacy? Is there a military or state security relationship to the means and motivations of surveillance? Which companies manufacture and sell surveillance software and equipment? This list goes on.

The case of surveillance drones [19] provides a rich example of the issues at play. Unmanned aerial vehicles were originally designed by the
monograph Privacy and New Technologies

The overarching point [of sousveillance] is to challenge the power dynamic inherent in surveillance to force transparency on organizations that conduct it.

U.S. military for battlefield reconnaissance. However, they have since been deployed in other contexts, such as along the Mexican and Canadian borders [20]. And even British police have expressed interest in using them domestically, to monitor drivers, protestors, and fly-tippers [21].

This phenomenon (known as ‘mission creep’ in the literature [22]) is the process by which technologies adopted for one aim are later repurposed to attain other policy goals.

Surveillance technology companies often operate and trade in secret; it has been difficult to discern the scale of the industry and the types of technology offered to law enforcement and intelligence agencies, making rigorous scholarly research in this area difficult. However, investigators and activists have begun to penetrate the secret conferences and venues in which these deals are made, and have subsequently begun to expose the trade. Much work remains to be done before this shadowy industry and its operations are understood.

9. Regulation and Governance
The regulation and governance of privacy and surveillance is hardly uniform [23]. Many countries offer constitutional privacy guarantees. Some don’t. Many countries have laws to regulate state and commercial collection and use of personal data. Others don’t [24].

Some jurisdictions observe laws regulating government access to certain types of communications data, as well as regulations for ‘lawful interception’: the circumstances under which it is legally permissible to intercept communications. Specific laws may also regulate specific types of data (e.g., health, financial or biometric information).

One problem with privacy and surveillance laws is that they’re often obsolete soon after they come into effect, as technology and innovation are so fast-moving. Even where relevant laws exist, they sometimes go unenforced. Enforcement typically requires a privacy, data protection or surveillance oversight commissioner to patrol the beat, and some countries (even those with privacy laws) don’t have such authorities in place. Where these agencies do exist, they’re often under-resourced or ineffective.

Many jurisdictions are responding to calls for privacy legislation, but privacy advocates must beware of so-called policy laundering: a phenomenon that Gus Hosein has examined in depth [25]. Countries without national policies or regulations for protecting privacy or limiting surveillance powers sometimes replicate bad or ineffective laws from other jurisdictions, thereby replicated their (in)effects. Another opportunity for advocates involves fighting for stronger constitutional protections for privacy, which will provide a safeguard when unambitious or ineffective laws are put in place.

10. Resistance
Among the most creative ideas on resistance to surveillance is the concept of sousveillance proposed by Steve Mann [26]. Sousveillance inverts surveillance to fix the gaze upon the organizations that are normally involved in monitoring subjects. The overarching point is to challenge the power dynamic inherent in surveillance to force transparency on organizations that conduct it. A popular manifestation of sousveillance is citizen use of camera-enabled mobile phones to capture police brutality, such as during the 2009 BART police shooting of Oscar Grant in Oakland, California.

Another interesting resistance project involves ‘hacking’ facial detection systems by using makeup and accessories to prevent computer algorithms from detecting one’s visage. Adam Harvey discovered that facial detection systems can be confused by applying makeup on certain parts of the face (see Figure 2) [27]. By distorting our appearance, we regain the ability resist surveillance, and protect our privacy, if we so choose.

My colleagues and I have explored the networks of resistance that emerge to surveillance projects. Whereas the majority of the academic literature on surveillance is focused on resistance relations between the watcher and the watched, we look at different ways of understanding the who and how of resistance to elaborate a multi-actor framework to better understand the complex resistance relationships that arise in local contexts [28].

11. Designing Privacy Technologies
Harvey’s project may be categorized as a ‘privacy-protecting’ technology project in that it aims to use tools (in this case, non-information technologies like makeup and eyeglasses) to impede facial detection. In general, privacy-protecting or privacy-enhancing technologies (PETs) provide a technical means to resist surveillance by increasing people’s control over their personal information, minimizing the personal data disclosed to private companies and the state, making privacy-invasive data processing more transparent, and anonymizing communications between parties.

In building their tools, designers of PETs are actively contesting and resisting the politics and values that Nissenbaum and Howe argue are embodied by systems of surveillance [29].

Figure 2. Low-tech Resistance to Facial Detection
Real-world examples of successful PETs include tools such as Tor, which provides a secure means to surf the web and communicate privately, and Ghostery, a browser plug-in that shows the tracking tags, web bugs, pixels and beacons that are embedded in web pages. The widespread diffusion of PETs would mark a major milestone in the advancement of privacy, but to date only a small minority of users has deployed them; there’s a high chance that you don’t use them, and it’s almost certain that grandma doesn’t.

So the real challenge is to get them built into the infrastructure. Why can’t the principles behind Tor be built into routers? Or the privacy and identity protecting principles [30] underlying Kim Cameron’s Laws of Identity [31] be built into national identification cards? It could be due to the complexity of these techniques, or because there’s a commercial and national security interest in ensuring systems that divide, identify, and reveal.

12. Identity, Pseudonymity, and Anonymity
One of the major privacy battles is the ongoing fight over identity policies online. For years it was possible to use the Internet anonymously, but the rise in trolling online, social anxieties about pedophiles lurking and grooming children in chat rooms, and exaggerated fears about terrorists using the Internet to plan attacks have resulted in a push to force users to be traceable and identifiable online at all times.

From this belief emerged the so-called nyms wars. On one side are online service providers, social networking sites, and even video gaming sites like Blizzard (makers of World of Warcraft [32]) that insist that people use their ‘real’ names on sites such as Google+. On the other side are academics, advocates, and activists who argue that there are many legitimate reasons for people to reserve the right to remain anonymous or to use pseudonyms online [33], such as political dissidents or anyone who faces analogue consequences for acceptable digital behavior. The good thing is, these are debates that academics have been engaging for years now. The list of recommended readings is extensive, but for starters I suggest the Lessons from the Identity Trail [34] edited volume and Whitley and Hosein’s Global Challenges for Identity Policies [35], which explores how the odd couple of politics and technology is sometimes forcibly wedded to address the complex challenges of identity policy.

13. Targeting, Tracking and Mobility
Another area in much need of engagement and advocacy is online targeting and tracking. The use of tracking technologies like cookies is fairly normal online. They can be innocuous, but as free services proliferate online more and more sites and applications are relying on tracking-dependent advertising revenue. These companies collect lots of information about users in order to be able to more accurately target advertisements. Users who are uncomfortable with being tracked may try to limit the number of cookies that are installed on their computers, but advertising networks have become more aggressive in their practices by relying on new techniques such as Flash-based cookies [36] and other methods [37] for covert but persistent tracking.

In the U.S. and elsewhere, there have been calls to introduce legislation prohibiting companies from tracking people online without consent but it remains to be seen what technologies would support these policies and how effectively these provisions could be enforced. This is a complex ecosystem, in which it is difficult to exercise total control over personal data (such as location). There are numerous actors involved in collecting and processing information and as it stands it’s difficult to discern where our data is flowing and how it’s being used.

Still, both online targeting and tracking and mobile privacy present exciting opportunities for activists to get involved in designing technologies (such as visualization tools to increase transparency around online surveillance practices, or through secure communications tools such as what Whisper Systems has developed for Android phones), or by working to improve policy and regulation in this space.

The great challenge is that as the Internet and mobile phone systems become increasingly structured, with necessary intermediaries (ISPs), new intermediaries (hardware providers, operating system developers), and services (applications, browsers, platforms), the emerging fragmented solutions will be ultimately unsuccessful.

14. What’s Missing?
Some very interesting research areas are inevitably missing from the above discussion. Surveillance labor is one: What’s the actual practice of monitoring video surveillance feeds like and what role do things like emotions [38] and stress [39] play in the job?

Surveillance methodology is another interesting avenue: How can we measure surveillance, both quantitatively and qualitatively, in order to understand whether or not it’s intensifying, and if so, how these changes are occurring? Kevin Haggerty has looked at these methodological conundrums [40].

The histories of different surveillance technologies also merit greater exploration. Simon Cole’s historical exposition of fingerprinting methods in forensics serves as a strong example of this kind of research. He shows how the taken-for-granted idea that our fingerprints are unique (and thus capable of individually identifying people) is actually an epistemologically complex artifact [41].

And what about surveillance failures? All too often we fixate on successful surveillance policies and systems, but we tend to forget all the projects that are abandoned, fizzle or fail. There’s a long list of surveillance technology that didn’t make it (remember Total Information Awareness [42]?). Why are such projects unsuccessful, and how are some apparently dead projects resuscitated and then incorporated into new initiatives (e.g., parts of Total Information Awareness still live on [43]?).

Acknowledgements
This primer was funded by a grant from the Information Program of the Open Society Foundations, with intellectual contributions from Daniel Bernhardt, Becky Hogge and Gus Hosein.
monograph Privacy and New Technologies

References


