HACKING THE PANOPTICON: DISTRIBUTED ONLINE SURVEILLANCE AND RESISTANCE

Benoît Dupont

ABSTRACT

Surveillance studies scholars have embraced Foucault's panopticon as a central metaphor in their analysis of online monitoring technologies, despite several architectural incompatibilities between eighteenth and nineteenth century prisons and twenty-first century computer networks. I highlight a number of Internet features that highlight the limits of the electronic panopticon. I examine two trends that have been considerably underestimated by surveillance scholars: (1) the democratization of surveillance, where the distributed structure of the Internet and the availability of observation technologies has blurred the distinction between those who watch and those who are being watched, allowing individuals or marginalized groups to deploy sophisticated surveillance technologies against the state or large corporations; and (2) the resistance strategies that Internet users are adopting to curb the surveillance of their online activities, through blocking moves such as the use of cryptography, or masking moves that are designed to feed meaningless data to monitoring tools. I conclude that these two trends are neglected by a majority of surveillance scholars because of biases that make them dismiss the initiative displayed by ordinary users, assess

Surveillance and Governance
Sociology of Crime Law and Deviance, Volume 10, 259–280

ISSN: 1521-6136/doi:10.1016/S1521-6136(07)00212-6

positive and negative outcomes differently, and confuse what is possible and what is probable.

The panopticon concept occupies a pivotal position in the field of surveillance studies. Michel Foucault's (1977) analysis of Bentham's total surveillance architecture has become a ubiquitous reference in the literature (Haggerty, 2006; Lyon, 2006), despite Foucault's deliberate lack of interest for the emerging technologies of his time (Haggerty & Ericson, 2000). A few years later, Thomas Mathiesen (1997) highlighted the limits of relying exclusively on the panopticon's metaphor in a "viewer society" where television lets the many see what the few are up to. Although these two major contributions still partly resonate with the current state of surveillance and continue to provide useful theoretical insights, I will argue in this chapter that their hegemonic influence (Haggerty, 2006) is becoming counterproductive to understand two trends related to surveillance in the online environment. The first trend can be defined (for lack of a better term) as the "democratization of surveillance", where cheap surveillance software and hardware is marketed to individual customers so that they can monitor the activities of their family, coworkers, neighbours, and even their favourite celebrity or their most despised politician. The second trend concerns the resistance to surveillance, where efforts are deployed by the subjects of surveillance to understand, reveal, mock, evade, and neutralize surveillance technologies through the collaborative power of socio-technical networks. Because of their incompatibility with the dominant panoptic and synoptic conceptual frameworks, these two trends have been underestimated and sometimes even ignored by surveillance scholars.

These two facets of contemporary surveillance will be examined in a very specific context: the omnipresent network of computers, servers, software, and services that make up the Internet. The Internet is now routinely used to exchange information of personal and public interest, to conduct financial transactions, to acquire goods and services of all kinds, and to spend time (or waste it, depending on the perspective) by playing online games, downloading music and movies, and managing social networks of friends and acquaintances. Its architecture is decentralized and distributed, making it at the same time very exposed and very resilient to failures and malfeasances. Its invention is recent, and when *Discipline and punish* was first published in French in 1975, ARPANET (the ancestor of the Internet) was still in its infancy (Mowery & Simcoe, 2002). At first sight, the Internet seems to embody the worst fears of a panoptic world: total surveillance can

be achieved at very low cost, making all exchanges traceable and significantly altering the notion of privacy (Lessig, 2006). As the Internet penetrates every aspect of our lives and the boundaries between the physical world and virtual world become irremediably blurred, we should be quite worried by these flows of digitized information that are used to create "data doubles" whose slightest alterations are constantly scrutinized (Haggerty & Ericson, 2000, p. 611). If one tool could manage to leverage the power of knowledge to govern the behaviour of a population, the Internet should figure among the top contenders (Graham & Wood, 2003). However, no matter how great the dystopian potential of the Internet is, it seems that it has not yet delivered its disciplinary promise. To be entirely fair, it has not liberated people from autocratic regimes either, as some of its most naïve promoters initially believed. One of the reasons for this lies in the "openness" paradox: while the technical protocols that underpin the Internet are public and standardized, therefore making surveillance relatively easy to carry out, the very same openness empowers application writers (programmers), who are free to design and distribute new tools of surveillance and resistance. For these reasons, the Internet seems like the perfect case study to assess the contemporary relevance of the panoptic and synoptic conceptual frameworks.

I do not contest the existence and growth of pervasive surveillance programmes run by governments that seek to unmask terrorist suspects before they strike or political opponents who criticize the abuses of authoritarian regimes. Nor do I want to minimize the impact of similar efforts by corporations that want to profile their customers better in order to increase their profit margins (Gandy, 1993; O'Harrow, 2005) or ensure the compliance of their employees (Associated Press, 2007). Recent developments in the United States – where the executive branch has authorized massive antiterrorist datamining initiatives despite their dubious constitutional legality (Eggen, 2007) – and elsewhere would make such a position untenable because of its complete disconnection from reality. However, a simple transfer of the panoptic model, so eloquently delineated by Foucault and refined by Mathiesen, does not provide a more accurate description of the reality of contemporary Internet surveillance. In the following sections, I will first explain why the panoptic and synoptic approaches provide an incomplete set of conceptual tools to analyze the proliferation of surveillance capacities in the online world, before examining how these capacities have become available to a broad range of social actors and are also increasingly resisted with a certain degree of success by a growing body of activists and ordinary users. Finally, in the conclusion, I offer a

non-exhaustive list of biases that have, in my opinion, prevented a significant number of surveillance scholars from integrating the trends mentioned above in their existing work.

THE PANOPTICON: AN EXHAUSTED SURVEILLANCE METAPHOR?

Although this question might seem unnecessarily provocative, I would like to show in this section the perils of extending eighteenth century thinking, no matter how innovative it was at the time, to twenty-first century technologies. Foucault's work assumes a certain linearity in the development and refinement of surveillance techniques, "from a schemata of exceptional discipline to one of a generalized surveillance, [which] rests on a historical transformation: the gradual extension of the mechanisms of discipline throughout the seventeenth and eighteenth centuries" (Foucault, 1977, p. 209), ending in the formation of "the disciplinary society". This unrelenting expansion of the disciplines does not consider the possibility of disruptive technologies that would redefine how people watch each others and resist various efforts to monitor their activities.

Panoptic Features

Foucault's analysis of Bentham's panoptic prison emphasizes a number of features. The first innovation consists in the physical ordering of the cells in a ring, in the middle of which a focal point – the observation tower – affords a perfect view of all the inmates. Such a "hub-and-spoke" architecture allows a single warden to watch a large number of cells and creates a new economy of surveillance. The asymmetrical power relation created by this circular architecture is reinforced by the lighting arrangements that induce total and permanent visibility for the inmates, while the guardians are shielded behind blinds that make them invisible to the surveillance subjects. A third feature consists in the partition between cells. The solitude it creates AU :1 seeks to make the inmate "a subject of information, never a subject in communication" (Foucault, 1977, p. 200), to remove the opportunities for coordination that could lead to a "collective effect". The expected result is a more effective institution, where the concentration of power facilitates the observation, classification, comparison, and ultimately, management of subjects.

Beyond an erudite description of Bentham's model, Foucault's main argument resides in the idea that the panopticon "must be understood as a generalizable model of functioning; a way of defining power relations in terms of the everyday life of men" (Foucault, 1977, p. 205). It is an ideal-type, "the diagram of a mechanism of power reduced to its ideal form; *its functioning, abstracted from any obstacle, resistance or friction*, must be represented as a pure architectural and optical system: it is in fact a figure of political technology that may and must be detached from any specific use" (Foucault, 1977, p. 205, my emphasis). Hospitals, military units, schools, or workshops were other places where Foucault identified panoptic mechanisms at work, in a trend that he predicted would result in the emergence of a disciplinary society. This total theory of surveillance and discipline proved very appealing and was embraced by a number of scholars, who extended its application to public spaces – where CCTV systems have become ubiquitous, in the workplace or on the Internet, just to name a few. While their interpretation of panopticism varies greatly (Lyon, 2006; Simon, 2005), they all implicitly subscribe to the idea of a power asymmetry between a small group of elite supervisors exercising a monopoly on surveillance tools, and a large mass of unsuspecting or passive individuals whose interests seem to rarely transcend their obsession for consumption (Bauman, 2000).

This hierarchical model of surveillance was famously challenged by Thomas Mathiesen, who introduced the concept of synopticism in his article on the "viewer society" (Mathiesen, 1997). Mathiesen reminds Foucault's readers that a significant piece of the contemporary surveillance puzzle is missing from the master's account:

> We have seen the development of a unique and enormously extensive system enabling *the many to see and contemplate the few*, so that the tendency for the few to see and supervise the many is contextualized by a highly significant counterpart. I am thinking, of course, of the development of the total system of the modern mass media. (Mathiesen, 1997, p. 219)

However, far from disagreeing with Foucault's conclusions, Mathiesen insists on the reciprocal functions of the panopticon and the synopticon, which are to control and discipline the "soul", ending his article on a very pessimistic note. Although he calls for political resistance as a moral imperative, his prognosis is very gloomy, and the Internet is merely seen as another media reproducing a familiar pattern of domination and oppression through surveillance and preformatted choices.

What is striking in this very severe judgement, which also resonates in many panoptic studies that extend Foucault's reasoning to computer

technologies (Poster, 1990; Sewell & Wilkinson, 1992; Gandy, 1993), is that it transposes the rock and mortar architecture of the prison to the structure of the Internet, built on wires and bits. A more careful examination of the Internet's structural features should however introduce a dose of relativism and open up new avenues of enquiry for the study of contemporary surveillance practices. In that respect, Yochai Benkler's book on "the wealth of networks" (2006) offers one of the most detailed accounts of the Internet's structural and institutional features, as well as a consideration of their impact on political and cultural freedoms.

The Internet as an Anti-Panopticon

Where the panopticon and synopticon adopt the "one-way, hub-and-spoke structure, with unidirectional links to its ends" (the periphery in the case of the former, the centre for the latter), the Internet is built as a decentralized and "distributed architecture with multidirectional connections among all nodes in the networked information environment" (Benkler, 2006, p. 212). This distribution of ties allows members of the network (machines and individuals) to access and communicate with other members through a large number of simultaneously available paths that very rarely transit through a single central node. This is due to the fact that the concept of centrality is by definition excluded from the architecture of the Internet to increase its resilience in case of a major failure of the central node. In this model of information management, it is much harder for a central authority to control the flow of data than in a panoptic environment, while at the same time, it becomes much easier for a myriad of actors to observe and monitor their peers, since the distribution of ties also creates a hyper-connectivity conducive to the multilateralization of surveillance. So, while the panoptic and synoptic models placed the emphasis on "the fact that the disciplines use procedures of partitioning and verticality, that they introduce, between the different elements at the same level, as solid separations as possible, that they define compact hierarchical networks, in short, that they oppose to the intrinsic, adverse force of multiplicity the technique of the continuous, individualizing pyramid" (Foucault, 1977, p. 220), the Internet functions under entirely different premises. It connects people and let them form horizontal networks – largely independent from governments – that moderate the distribution of power instead of reinforcing its concentration (Lessig, 2007, p. 274). AU :2

This is not to say that the Internet is devoid of architectures of control: governments and businesses around the world spend considerable amounts of money to design surveillance systems able to tell them who is doing what, with whom, and from where on the Internet (Lessig, 2006, p. 38). But these technologies are not exclusive to a restricted group of supervisors. They are becoming increasingly accessible to individual users and fulfill a number of functions that range from the noble to the mundane, and the disciplinary to the playful. They must also contend with a number of resistance technologies and behaviours that thrive in the Internet environment because of its very un-panoptic architecture.

THE DEMOCRATIZATION OF SURVEILLANCE

The term democratization refers to the broadening accessibility of online surveillance through a plurality of tools and services that could previously only be afforded by governments and large companies. This trend reverberates both in the private and public spheres, and corresponds to a wide range of rationalities sustained by business-oriented ventures, non-governmental organizations (NGOs), and social units such as families and groups of friends. Low barriers of entry to the world of online surveillance are responsible for this democratization. Contrary to other mass media such as television or newspapers, the marginal costs for the distribution of information on the Internet are very low, because expensive proprietary infrastructure such as satellites, fibre-optic cables, printing presses, and delivery routes are not required (Benkler, 2006). All providers of Internet services share the same infrastructure and the same data transfer protocols, also known as TCP/IP (Lessig, 2006, pp. 143–146). Therefore, large investments in capital assets are not required to start disseminating information, as millions of bloggers have found out. Most of the costs incurred by new service providers are associated with the collection and sorting of data, or the development of new methods to collect and sort data more effectively or more efficiently. For example, the success of the very popular Google search engine can be attributed to the superior quality of its ranking algorithm, making the results it displays at the top of its page more relevant than those of its competitors. Once data or information has been processed, it can be distributed or accessed on a large-scale at little or no additional cost.

This combination of openness and cheap means of distribution constitutes a powerful incentive to innovations fuelled by entrepreneurs and social activists alike. These innovations can be categorized in two

groups. The first group merges off-line observation technologies with online dissemination tools, while the second group is entirely made up of online technologies that are used to collect and distribute data. Among the observation technologies mobilized by the first group, we find digital photography and video recording, remote sensing, geographical information systems, human input, and social engineering. The following examples will provide a better idea of the democratization processes at work.

Online Diffusion of Content Collected by Off-Line Observation

YouTube[1] is probably the best-known video-sharing website, with an estimated monthly audience of 20 million people and 100 million video downloads per day. The company, whose slogan is "broadcast yourself", adds more than 65,000 videos every day to its library. Users of the site directly post these short segments with very limited interference from YouTube employees, whose number does not exceed 30 people (Reuters, 2006). Thousands of contributors find there a platform to share contents produced by the explosion of video-capable consumer devices such as camcorders, computer webcams, or mobile phones. Although YouTube and other less successful video-sharing websites are primarily promoting the entertainment aspect of their services, many videos uploaded on their servers have a distinctive surveillance flavour: shopkeepers or homeowners are routinely making surveillance tapes of burglars breaking into their property available in the hope that it will increase their chances of being arrested (Rodriguez, 2007), grainy videos capturing police brutality incidents or blatant instances of corruption are uploaded at regular intervals,[2] and politicians uttering racial slurs or contradicting themselves shamelessly in semi-private functions are also bound to find their duplicity exposed to an audience of millions within hours, with very limited opportunities for damage control.[3] The miniaturization of video recording devices and the ubiquity of Internet access points, even in conflict zones, also allow anyone with a connected computer to remotely experience the ferocity and confusion of close quarter combat: Iraqi insurgents and US troops alike profusely post uncensored videos of their deadly encounters, providing far bleaker pictures of the conflict than the sanitized versions offered by the main television networks. YouTube and its edgier competitors LiveLeak and Dailymotion return thousands of results for search terms such as "Iraq war", "insurgency", "sniper", or "IED" (improvized explosive devices).

At the other end of the spectrum, macro-observation technologies such as remote sensing and geographical information systems applied to the Internet information economy can foil the efforts deployed by governments and large corporations to conceal some of their most questionable activities. Google and Microsoft offer through their Google Earth and Virtual Earth services high resolution geocoded satellite pictures of the planet that can been used for surveillance purposes, despite the fact that the data provided is usually a few weeks to three years old.[4] These very popular tools are free to use, and Google claims that more than 100 million people have downloaded the software needed to access its imagery (Meyer, 2006). The primary use of these tools involves the first-hand observation of what past official maps deliberately omitted (Monmonier, 1991), hidden behind high walls, or too remote to be accessed by any other means. The Cryptome website offers, for example, a series of detailed "eyeball" pictures[5] that expose sensitive infrastructures such as military bases, intelligence agencies' headquarters, politicians', and company executives' residences, in an effort to dispel the myths surrounding these secretive places. Anyone with a connection to the Internet can comb the millions of satellite pictures available online in order to satisfy their idiosyncratic curiosity. Some people use this capacity to track the latest nuclear submarine launched by the Chinese navy[6] while others are just as happy having a peek at the houses of the rich and famous[7] or the places they will visit during their next vacation. NGOs are also enlisting Google Earth to call attention to civil wars and humanitarian disasters such as Darfur. Amnesty International has launched a campaign called "eyes on Darfur" that uses satellite imagery to present the extent of violence committed in this inhospitable part of the world and let Internet users "monitor [12] high risk villages [to] protect them from further attack" in what the NGO describes as the "global neighbourhood watch".[8] The United States Holocaust Memorial Museum offers a similar experience on its website, but on a much larger scale. It plans to use these satellite pictures to build an online "global crisis map" of emerging genocides or crimes against humanity, which would allow activists, journalists, and citizens to access and share information more quickly.[9] At the illegal end of the spectrum, some terrorists have even embraced these surveillance tools to identify possible targets and their vulnerabilities (Harding, 2007), an approach explicitly acknowledged by Google on its website when it describes how homeland security agencies can leverage the power of Google Earth to conduct "critical infrastructure vulnerability assessment" and "pattern visualization of surveillance data" for $ 400 a year.[10]

A more significant outcome of these online technologies derives from the capacity to combine satellite pictures and maps with other types of digital data provided by sensors such as mobile phones, or generated by users themselves. These new applications are known as "mashups" and are made possible by open and easy-to-use programming formats and tools (Eisenberg, 2007) that fuse layers of information into a single file, adding value to the original pool of diverse data. Some businesses incorporate mashups to the affordable surveillance tools they market, such as mobile phone companies that offer handsets equipped with global positioning systems and let their customers (usually parents) track online the movements of the person carrying the phone (usually a child) (Pogue, 2006). Beyond the rise of Big Mother and Big Father, mashups also assist citizens in their efforts to gain a more detailed awareness of their immediate environment. While interactive crime maps that let online users create personalized outputs based on criteria such as type of crime, zip code, location, or even transport route,[11] are popular in the United States, Europeans seem more interested in monitoring the location of speed and red light cameras. The SCDB website[12] claims to maintain a database of 18,000 cameras scattered all over Europe, whose coordinates are updated by road users (Big Driver?).

Online Surveillance of Online Activities

In the previous examples, the Internet was used as a mediator by millions of connected supervisors who access dispersed real-world data, then modify, aggregate, and disseminate it for their own benefit, for altruistic motives, or in some instance for criminal gain. The same process applies to the surveillance of online activities, which cannot structurally be monopolized by governments or large corporations. As the underlying rationale is fairly similar, I will only use three examples (two lawful, the last one criminal) to show how this works. The first example demonstrates how travellers who book their trips online can harness the power of self-surveillance to extract cheaper airfare and hotel room rates from companies that have developed predatory pricing systems based on consumers' surveillance. This practice is known in the tourism industry and in other sectors that deal in perishable items as "yield pricing" or "yield management" (Desiraju & Shugan, 1999) and involves the dynamic allocation of discounts so that revenues are maximized for each flight or room sold (Borenstein & Rose, 1994, p. 655). The complexity of this pricing system can only be managed by computers

that constantly adjust prices to encourage purchases when sales are going slowly and maximize profits when the demand is strong, sometimes resulting in airfares that vary from one minute to another. Obviously, it creates a form of discrimination between consumers who pay fares that vary substantially for the same service, since they do not have access to the same data and tools on which to base their decision. The Internet resolved this informational asymmetry by creating a forecasting market that monitors the highs and lows of airfares or hotels rates. Services such as Farecast[13] or Kayak[14] use datamining techniques to comb the wild fluctuation of thousands of airfares over long periods of time and advise customers on the best purchasing strategy (wait or buy). Although they are applied to a fairly mundane activity, these tools should be understood as highly disruptive by nature. They bring meta-surveillance capacities to individuals who can deploy their own sophisticated technologies to uncover the routine surveillance to which they are submitted by large corporations.

The second example also illustrates how the democratization of surveillance can be used to expose the online activities of powerful interests. Whether it represents an improvement or not, the online collaborative encyclopedia Wikipedia[15] has become in a matter of years a source of reference material for millions of Internet users who also contribute to its entries. Content accuracy is a major issue (Giles, 2005), especially for controversial issues where conflicting interpretations of an event or someone's actions can lead to defamatory or plainly dishonest comments (Kolbitsch & Maurer, 2006). Government agencies that seek to defend their record on contested policy decisions or want to obscure their mistakes are tempted, in that context of openness, to edit entries that refer to them. Large corporations and NGOs might also use Wikipedia as a public relations tool to downplay their responsibility in embarrassing scandals or inflate their contributions to society. Unfortunately for them, the same surveillance tools that are used to undermine privacy and authenticate the identity of every Internet user can also be used to identify (to a certain extent) who has made changes on any given Wikipedia entry. This capacity has always been available to computer-savvy users through what is known as an IP tracer or IP locator. The term IP stands for Internet Protocol and refers to the addressing system that allows data to be sent to the right machine on the network. IP addresses are unique identifiers, and although they are not allocated on a geographical basis, it is still fairly easy to locate a user based on publicly available IP address tables (Lessig, 2006, p. 59). Hence, talented programmers can develop an IP mapping application that integrates seamlessly with another web application. Virgil Griffith, the designer of

WikiScanner,[16] is one of those talented programmers. His online search engine lets users find out which organizations are the most active Wikipedia editors. Thousands of changes made by people working for government agencies such as the US Department of Homeland Security, the Pentagon, or the CIA; companies such as Wal-Mart or Exxon; NGOs such as the American Civil Liberties Union (ACLU) or the Electronic Frontier Foundation or even religious entities such as the Vatican or the Church of Scientology are retrievable. While some of them are the results of bored employees taking a break to update a page that relates to their personal interests (in itself a form of resistance), many others are linked directly to attempts by these organizations to anonymously shape their image. The openness that characterizes the Internet's architecture renders these clandestine efforts much easier to detect, providing sufficient incentives exist for someone to provide monitoring tools and for users to take advantage of them.

The surveillance tools described above are not isolated or exceptional, but the democratization trend is not synonymous with equal access to surveillance resources either. The barriers to the deployment of highly intrusive online surveillance technologies are not financial resources, but instead technical skills. While governments have rapidly expanded their online surveillance capacities since 9/11, criminal actors have also been busy deploying their own elaborate webs of surveillance. Botnets (the contraction of software robot and network) are computer networks made up of compromised machines (called zombies) that have been infected by viruses or other malicious software and that can, as a result, be monitored and controlled remotely without the knowledge of their rightful owners. These botnets are used by hackers (called botmasters in this instance) to send spam, commit click fraud,[17] or launch large-scale attacks against websites in order to shut them down or extort money from their operators to stop the attacks.[18] Botnets are routinely used to perform scans of their host machines. With some of them including more than a million compromised computers (Gaudin, 2007) and conservative studies evaluating botnet infection at 11% of all computers connected to the Internet (Abu Rajab, Zarfoss, Monrose, & Terzis, 2006), their mass surveillance potential is not hard to imagine. In this last example, surveillance is no more horizontal and democratic than it is vertical or centralized, and the panoptic model can only be of limited assistance to analyze the distributed structure of supervision, and its disconnect from any disciplinary and social sorting project (Haggerty & Ericson, 2000; Lyon, 2006; Haggerty, 2006). Social and

technical factors such as the plurality of functions associated with the monitoring of others' online activities, regulatory frameworks, new business models, computer skills of Internet users, and the open or faulty code of communication protocols all play an important role in the adoption of online surveillance technologies. Unfortunately, we have barely begun examining these variables' empirical architecture, which also influence the numerous resistance strategies employed by those who want to defend their privacy from the omnipresent surveillance of the state, their family and friends, or computer hackers.

RESISTANCE TO ONLINE SURVEILLANCE

In line with Foucault's lack of interest for resistance as a counteracting force to the oppressive panoptic gaze, many modern surveillance scholars have dismissed the possibility of collective neutralization and sabotage efforts or have been ambivalent about them, at best (Gandy, 1993, p. 147; Campbell & Carlson, 2002, p. 603), despite clear signs that they are not isolated occurrences (Bain & Taylor, 2000; Timmons, 2003; Lyon, 2004, Poster, 2005; Bogard, 2006, p. 101). Acts of resistance in surveillance studies are often presented as individual and localized efforts (Haggerty & Ericson, 2006, p. 18) that produce partial and temporary victories (Gilliom, 2006, p. 115) and merely reinforce the effectiveness of surveillance through an escalation process. There are, however, many ways for the subjects of surveillance to reclaim their privacy and autonomy, as Gary Marx (2003) so compellingly demonstrated. Although the eleven resistance strategies he describes in his article apply more or less to online surveillance, two of them will be considered in greater detail, and from a collective rather than an individual perspective. These strategies are: blocking moves and masking moves.

Cryptography as a Blocking Move

Blocking moves refer to the process that seeks "to physically block access to the communication" (Marx, 2003, p. 379). Blocking moves are inconceivable in the panoptic world, since partitions prevent subjects from contacting each others, whereas on the Internet, where messages transit through multiple paths, they become an essential tool to ensure the safety of

communications. Cryptography is perhaps one of the oldest blocking moves. It can be defined as:

> A transformation of a message that makes the message incomprehensible to anyone who is not in possession of secret information that is needed to restore the message to its normal *plaintext* or *cleartext* form. The secret information is called the *key,* and its function is very similar to the function of a door key in a lock: it unlocks the message so that the recipient can read it. (Diffie & Landau, 1998, p. 13)

Cryptography has a long history that dates back to the invention of writing and played an instrumental role in several military conflicts (Singh, 1999; Pincock, 2006). Yet, its impact on Internet surveillance is rarely considered, despite the fact that the need to safeguard online financial transactions makes it one of the most widely used online privacy tools. If encryption procedures were mainly used by spies and diplomats before the advent of the Internet, the computing power available in each PC today is sufficient to produce scrambled messages that would foil the most determined code breakers. Since Philip Zimmermann made his Pretty Good Privacy (PGP) encryption software available on the Internet in 1990 and won his legal battle with the US Department of Justice, anyone who is not a mathematician or programmer can still enjoy the benefits of unbreakable encryption and defeat the most sophisticated surveillance technologies (Diffie & Landau, 1998). For example, terrorist organizations, pedophiles, and computer hackers have been known to use off-the-shelf or homemade encryption tools to conceal their unlawful activities (Denning & Baugh, 2000). Encryption is sometimes used by human rights organizations who want to protect their correspondents in authoritarian regimes. Although most popular e-mail programs such as Outlook or Thunderbird can send and receive encrypted emails, very few people actually use this facility. An Internet user survey conducted by Garfinkel, Margrave, Schiller, Nordlander, and Miller (2005) shows that 68% of people in their sample ($N = 417$) were either unaware that encryption was available on their e-mail client or did not know what cryptography was. Hence, despite the fact that cryptography is widely available at virtually no charge to Internet users, resistance to online surveillance is informed by other factors than purely technical considerations. A study of political activists opposing US administration policies in the post-9/11 environment shows that users balance the need for secrecy with a reluctance to fall into what they perceive as a paranoid or abnormal state of mind (Gaw, Felten, & Fernandez-Kelly, 2006). Systematic resistance that applies indiscriminately to mundane and highly sensitive content is experienced as a mental burden denoting an

unbalanced personality, while selective resistance is described by one respondent as similar to healthy eating and exercise: people know it is the right thing to do, but they are not always doing it themselves (p. 594). What these informed users tell us is that they resort to blocking moves with parsimony, maintaining a much more complex rapport to resistance than initially assumed by surveillance scholars.

Distributed Masking Moves

Masking moves that allow users to surf the web anonymously are more widespread than blocking moves. One reason that might explain this difference is that the former take full advantage of the distributed architecture of the Internet by establishing virtual networks of trust (Tilly, 2005). These resistance networks thwart surveillance attempts by randomly routing the information their members want to send or receive through other members of the network, thereby making it impossible for supervisors to know who is effectively communicating with whom and about what. TOR (The Onion Router), Freenet, and Psiphon[19] are examples of popular masking tools that are freely available for download and use on the Internet. Freenet's homepage claims that its software was downloaded more than two million times, and TOR's user base is said to reach hundreds of thousands, mainly from the United States, Europe, and China (Zetter, 2007). Although these programs differ slightly at the technical level, their overall approach is similar. Once people have installed them on their computer, a portion of their hard drive is automatically encrypted and secure connections are established with other computers that run the same software when the user logs on the Internet. All communications transit seamlessly through other nodes of the trust network before they are allowed into the more open and easily monitored part of the Internet. Attributing a particular online behaviour to a specific machine, and hence to its owner or operator, becomes a fruitless endeavour since complex algorithms are used to blur the patterns of data that enter and exit the trust network. What makes this type of trust network different from the more traditional ones described by Tilly (2005) is that it is scalable and does not require its members to share the same objectives. It is scalable in the sense that the more members these masking tools can enlist, the more effective they will be, while traditional trust networks expose themselves to failure and malfeasance when their membership becomes too large and difficult to manage. The second feature of these virtual trust networks is that credentials are allocated on a

technological basis (the willingness to encrypt and relay encrypted communications with no control over the contents being transmitted) more than on ethno-religious traits or shared social or political interests, making strange bedfellows in the process. Even though they are primarily destined to privacy and anti-censorship activists, diplomatic missions, intelligence agencies, and armed forces – including from authoritarian regimes such as Iran – also make intensive use of these free masking tools (Zetter, 2007), a good indicator of the trust these surveillance organizations place in them to protect their sensitive information against their counterparts.

Less drastic masking moves involve the manipulation by consumers of registration and search data in order to minimize the generation of profiles based on viewing patterns and datamatching techniques. The free online service BugMeNot[20] (BMN) offers to bypass the registration process that is compulsory to enter many websites by providing its users access to a database made up of active accounts (usernames and passwords) obtained by submitting fake socio-demographic details. BMN also provides disposable e-mail addresses that can be used for twenty-four hours as an alternative to disclosing real e-mail address to online merchants and data-brokers. Because the online interface allows users to directly submit new accounts and retrieve passwords from the database, there is a positive correlation between the number of users and the utility they derive from this service. As of September 2007, BMN provided accounts to more than 175,000 websites. Another interesting initiative is TrackMeNot[21] (TMN), a little program written by two New York University professors.[22] This application is used whenever the Firefox browser[23] accesses Internet search engines such as Google, AOL, Yahoo, and MSN. These websites keep track of all the searches performed by individual users in order to return context or location-relevant advertisements to accompany search results (Barbaro & Zeller, 2006). TMN uses an obfuscation strategy to drown real search queries in a cloud of randomly generated queries that makes profiling considerably more difficult and much less accurate, if not totally meaningless. The inventors of TMN actually acknowledge on their webpage that Gary Marx's article "A tack in the shoe" (2003) partly inspired their application.

CONCLUSION

The reified panoptic metaphor that dominates the field of surveillance studies appears increasingly detached from the complex reality of online monitoring (Boyne, 2000; Haggerty, 2006). Through a detailed analysis

of several diverse meta-surveillance and resistance technologies, I have attempted to expand the register of legitimate research questions on this issue. For example, how do some disruptive technologies concretely modify the underlying distribution of knowledge and power in the surveillant assemblage (Haggerty & Ericson, 2000)? How are expanding monitoring technologies appropriated by people and institutions for unexpected uses? What are the individual, social, political, economical, and technological factors that impact on resistance or constrain the effectiveness of surveillance? Can resistance be integrated to the study of surveillance, or should it be treated as a separate subject? These questions challenge the panoptic framework, but they also have the potential to make it more relevant to twenty-first century technological conditions. To be answered, they require a more grounded knowledge of the actual interactions between those who watch, the machines and infrastructure they design and use to carry out their surveillance, the people being watched and the flows of data that are generated as a result. These connections involving humans, machines, and places are easier to map in high-technology environments, because they leave behind a profusion of traces or markers, but it cannot be done without first abandoning the paranoid and megalomaniac tendencies the panopticon so often fuels (Latour, 2005).

While compiling example upon example of distributed surveillance and widespread resistance, I could not help wonder why so many surveillance scholars had carefully avoided this less travelled path. In an important contribution, Kevin Haggerty (2006) offers some interesting hypothesis to explain this reluctance, such as the critical thinking tradition of surveillance scholars, their simplified understanding of Foucault's integral intellectual legacy, a focus on human surveillance that neglects human/technological hybrids, and a methodological approach that overemphasizes discourse and document analysis to the detriment of more grounded empirical data. This last trait makes surveillance scholars overly dependent on the public transcripts that explain power relations between subjects and supervisors. Unfortunately, the official story is rarely the whole story, and hidden transcripts that can be defined as "offstage speeches, gestures, and practices that confirm, contradict, or inflect what appears in the public transcripts" (Scott, 1990, p. 4) should also be studied. However, the critical posture or methodological choices made by surveillance scholars cannot entirely explain the lack of interest for the "arts of resistance" and their impact on the governance of surveillance.

I offer an additional interpretation inspired by Gary Marx's (2007) techno-fallacies article and the heuristics' theory of Tversky and Kahneman

(1982). Just like technophiles often succumb to the false belief that there is a technological fix for every security problem, surveillance scholars (as an epistemic community, not as individuals) are not immune to biases that lead them to assume that the monitoring technologies embedded in virtually every aspect of our lives are a clear indicator of our inexorable fall into a 1984 reality. Three biases are particularly salient in this belief system. The first bias is the initiative bias, which leads people to attribute less initiative and less imagination to others than to themselves (Kahneman & Tversky, 1993, p. 3), especially if they belong to a lower socio-economic group. While surveillance scholars are able to offer elaborate narratives of the hidden power of the electronic panopticon and its significance, they frequently discount the interpretive capacities and agency of surveillance subjects and the resistance strategies that ensue. The loss aversion bias refers to the asymmetrical evaluation of positive and negative outcomes, where losses are systematically overestimated and gains are underestimated. This bias seems particularly pronounced "when the reference point is the status quo, and when retention of the status quo is an option" (Kahneman & Tversky, 1993, p. 14). This bias corresponds in surveillance studies to the reticence manifested toward the study of positive developments (Haggerty, 2006, p. 35) such as the accountability produced by meta-surveillance applications or the independence afforded to elderly patients by monitoring systems that let them stay at home. The tendency to predict widespread erosions of freedom has also been a prominent feature of surveillance studies, despite the lack of empirical and historical data to support this claim. Democracies have not crumbled since advanced monitoring technologies have invaded our lives, and the lack of sophisticated surveillance tools has never prevented authoritarian states to enroll thousands of informers to control internal dissent (Pfaff, 2001). Finally, the third heuristic is the probability bias whereby a confusion is made between what is possible and what is probable (Ohm, 2007). This bias is very closely connected with the previous one, because on contentious subjects such as surveillance and privacy, people tend to focus on disastrous outcomes and neglect the role played by randomness (Taleb, 2004), complexity, and contested rationalities (Espeland, 1998) among supervisors. Surveillance scholars frequently present what may happen as what will happen, obscuring the mechanisms that so often derail the best plans. Perhaps, the fact that Bentham's panopticon was actually never built and that the British government preferred instead to deport its prisoners to Australia, an open-air prison where convict supervision was deliberately kept at a minimum (Kerr, 1989;

Jackson, 1998), should serve as a reminder that dystopias are about as likely to materialize as utopias.

NOTES

1. http://www.youtube.com, accessed September 4, 2007.
2. See for example the string of videos showing Moroccan police officers receiving cash payments from truck drivers at http://www.youtube.com/watch?v=Afed8wvYwmc, accessed September 11, 2007.
3. Former US Republican senator George Allen (with presidential aspirations) lost his bid in the 2006 election after a video in which he called an aide to his opponent a «macaca» was made available on YouTube at http://www.youtube.com/watch?v=r90z0PMnKwI, accessed September 11, 2007.
4. See Google Earth help centre at http://earth.google.com/support/, accessed September 15, 2007.
5. http://eyeball-series.org/, accessed September 15, 2007.
6. http://www.fas.org/blog/ssp/2007/07/new_chinese_ballistic_missile.php, accessed September 16, 2007.
7. http://www.gearthhacks.com/dlcat25/Famous-Homes.htm, accessed September 16, 2007.
8. http://www.eyesondarfur.org/, accessed September 16, 2007.
9. http://www.ushmm.org/googleearth/projects/darfur/, accessed September 16, 2007.
10. http://earth.google.com/security.html, accessed September 16, 2007.
11. http://www.chicagocrime.org/; http://www.latimes.com/news/local/crime/homicidemap/; http://www.mapufacture.com/feeds/1000398-Oakland-Crime-Feed, all accessed September 16, 2007.
12. http://www.scdb.info/. It is one among others: see for example http://www.speedcameramap.co.uk/ and http://www.spod.cx/speedcameras.shtml for the United Kingdom, all accessed September 16, 2007.
13. http://www.farecast.com, accessed September 22, 2007.
14. http://www.kayak.com, accessed September 22, 2007.
15. http://www.wikipedia.org, accessed September 22, 2007.
16. http://wikiscanner.virgil.gr/, accessed September 22, 2007.
17. A practice where online advertisers are charged for clicks on banners that originate from computer software and not legitimate users interested in their product.
18. They are known as DDoS or distributed denial of service attacks.
19. http://tor.eff.org/, http://freenetproject.org, and http://psiphon.civisec.org/, all accessed September 25, 2007.
20. http://www.bugmenot.com, accessed September 25, 2007.
21. http://mrl.nyu.edu/~dhowe/trackmenot/, accessed September 25, 2007.
22. Daniel C. Howe, from the Media Research Lab and Helen Nissenbaum from the Culture and Communication department.
23. Unfortunately, the program is not available with the most popular Microsoft Explorer browser.

REFERENCES

Abu Rajab, M., Zarfoss, J., Monrose, F., & Terzis, A. (2006). A multifaceted approach to understand the botnet phenomenon. In: P. Barford (Ed.), *Proceedings of the 6th ACM SIGCOMM on Internet measurement* (pp. 41–52). New York, NY: ACM Press.

Associated Press. (2007). New breed of 'compliance software' makes office computer monitoring more sophisticated. *Technology Review*, published August 20, 2007, retrieved August 21, 2007, from http://www.technologyreview.com/Wire/19271/page1/

Bain, P., & Taylor, P. (2000). Entraped by the 'electronic panopticon'? Worker resistance in the call centre. *New Technology, Work and Employment*, *15*(1), 2–18.

Barbaro, M., & Zeller, T. (2006). A face is exposed for AOL searcher no. 4417749. *The New York Times*, published August 9, 2006, retrieved September 25, 2007, from http://www.nytimes.com/2006/08/09/technology/09aol.html

Bauman, Z. (2000). *Liquid modernity*. Cambridge: Polity Press.

Benkler, Y. (2006). *The wealth of networks*. New Haven, CT: Yale University Press.

Bogard, W. (2006). Surveillance assemblages and lines of flight. In: D. Lyon (Ed.), *Theorizing surveillance: The panopticon and beyond* (pp. 97–122). Cullompton: Willan Publishing.

Borenstein, S., & Rose, N. (1994). Competition and price dispersion in the U.S. airline industry. *The Journal of Political Economy*, *102*(4), 653–683.

Boyne, R. (2000). Post-panopticism. *Economy and Society*, *29*(2), 285–307.

Campbell, E., & Carlson, M. (2002). Panopticon.com: Online surveillance and the commodification of privacy. *Journal of Broadcasting & Electronic Media*, *46*(4), 586–606.

Denning, D. E., & Baugh, W. E. (2000). Hiding crimes in cyberspace. In: D. Thomas & B. D. Loader (Eds), *Cybercrime: Law enforcement, security and surveillance in the information age* (pp. 105–131). London: Routledge.

Desiraju, R., & Shugan, S. (1999). Strategic service pricing and yield management. *Journal of Marketing*, *63*(1), 44–56.

Diffie, W., & Landau, S. (1998). *Privacy on the line: The politics of wiretapping and encryption*. Cambridge, MA.: MIT Press.

Eggen, D. (2007). Lawsuits may illuminate methods of spy program. *The Washington Post*, August 14, p. A01.

Eisenberg, A. (2007). Do the mash (even if you don't know all the steps). *The New York Times*, September 2, p. 5.

Espeland, W. (1998). *The struggle for water: Politics, rationality and identity in the American Southwest*. Chicago, IL: The University of Chicago Press.

Foucault, M. (1977). *Discipline & punish: The birth of the prison*. New York, NY: Pantheon Books.

Gandy, O. H. (1993). *The panoptic sort: A political economy of personal information*. Boulder, CO: Westview Press.

Garfinkel, S., Margrave, D., Schiller, J., Nordlander, E., & Miller, R. (2005). How to make secure email easier to use. In: W. Kellogg & S. Zhai (Eds), *Proceedings of the SIGCHI conference on human factors in computing systems* (pp. 701–710). New York, NY: ACM Press.

Gaudin, S. (2007). Storm worm botnet more powerful than top supercomputers. *Information Week*, published September 6, 2007, retrieved September 23, 2007, from http://www.informationweek.com/story/showArticle.jhtml?articleID=201804528

Gaw, S., Felten, E., & Fernandez-Kelly, P. (2006). Secrecy, flagging and paranoia: Adoption criteria in encrypted e-mail. In: R. Grinter, T. Rodden, P. Aoki, E. Cutrell, R. Jeffries & G. Olson (Eds), *Proceedings of the SIGCHI conference on human factors in computing systems* (pp. 591–600). New York, NY: ACM Press.

Giles, J. (2005). Internet encyclopedias go head to head. *Nature*, *438*(7070), 900–901.

Graham, S., & Wood, D. (2003). Digitizing surveillance: Categorization, space, inequality. *Critical Social Policy*, *23*(2), 227–248.

Haggerty, K. D. (2006). Tear down the walls: On demolishing the panopticon. In: D. Lyon (Ed.), *Theorizing surveillance: The panopticon and beyond* (pp. 23–45). Cullompton: Willan Publishing.

Haggerty, K. D., & Ericson, R. V. (2000). The surveillant assemblage. *The British Journal of Sociology*, *51*(4), 605–622.

Haggerty, K. D., & Ericson, R. V. (2006). The new politics of surveillance and visibility. In: K. D. Haggerty & R. V. Ericson (Eds), *The new politics of surveillance and visibility* (pp. 3–25). Toronto: University of Toronto Press.

Harding, T. (2007). Terrorists 'use Google maps to hit UK troops'. *The Telegraph*, published January 13, 2007, retrieved September 16, 2007, from http://www.telegraph.co.uk/news/

Jackson, R. V. (1998). Jeremy Bentham and the New South Wales convicts. *International Journal of Social Economics*, *25*(2/3/4), 370–379.

Kahneman, D., & Tversky, A. (1993). *Conflict resolution: A cognitive perspective*. Toronto: University of Toronto.

Kerr, J. (1989). Panopticon versus New South Wales. *Fabrications : The Journal of the Society of Architectural Historians, Australia and New Zealand*, *1*, 4–32.

Kolbitsch, J., & Maurer, H. (2006). The transformation of the web: How emerging comm unities shape the information we consume. *Journal of Universal Computer Science*, *12*(2), 186–213.

Latour, B. (2005). *Reassembling the social: An introduction to actor-network-theory*. Oxford: Oxford University Press.

Lessig, L. (2006). *Code version 2.0*. New York: Basic Books.

Lyon, D. (2004). Globalizing surveillance: Comparative and sociological perspectives. *International Sociology*, *19*(2), 135–149.

Lyon, D. (2006). 9/11, synopticon and scopophilia: Watching and being watched. In: K. D. Haggerty & R. V. Ericson (Eds), *The new politics of surveillance and visibility,* (pp. 35–54). Toronto: University of Toronto Press.

Marx, G. T. (2003). A tack in the shoe: Neutralizing and resisting the new surveillance. *Journal of Social Issues*, *59*(2), 369–390.

Marx, G. T. (2007). Rocky Bottoms: Techno-fallacies of an age of information. *International Political Sociology*, *1*(1), 83–110.

Mathiesen, T. (1997). The viewer society: Michel Foucault's 'Panopticon' revisited. *Theoretical Criminology*, *1*(2), 215–234.

Meyer, D. (2006). Google, Microsoft vie for earth domination. *CNET News.com*, published September 12, 2006, retrieved September 15, 2007, from http://www.news.com/

Monmonier, M. (1991). *How to lie with maps*. Chicago, IL: The University of Chicago Press.

Mowery, D. C., & Simcoe, T. (2002). Is the Internet a US invention? An economic and technological history of computer networking. *Research Policy*, *31*(8–9), 1369–1387.

O'Harrow, R. (2005). *No place to hide*. New York: Free Press.

Ohm, P. (2007). The myth of the superuser: Fear, risk, and harm online. *University of Colorado Law Legal Studies Research Paper No. 07-14*, retrieved September 28, 2007, from http://www.ssrn.com/abstract=967372

Pfaff, S. (2001). The limits of coercive surveillance: Social and penal control in the German Democratic Republic. *Punishment & Society*, *3*(3).

Pincock, S. (2006). *Codebreaker: The history of codes and ciphers, from the ancient pharaohs to quantum cryptography*. New York, NY: Walker & Company.

Pogue, D. (2006). Cellphones that track the kids. *The New York Times*, December 21, 2006, C1.

Poster, M. (1990). *The mode of information: Poststructuralism and social context*. Chicago, IL: The University of Chicago Press.

Poster, M. (2005). Hardt and Negri's information empire: A critical response. *Cultural Politics*, *1*(1), 101–118.

Reuters. (2006). YouTube serves up 100 million videos a day online. *USA Today*, published July 16, 2006, retrieved on September 3, 2007, from http://www.usatoday.com/tech/news/2006-07-16-youtube-views_x.htm

Rodriguez, G. (2007). YouTube vigilantes. *Los Angeles Times*, published August 6, 2007, retrieved September 11, 2007, from http://www.latimes.com/news/opinion/

Scott, J. C. (1990). *Domination and the arts of resistance: Hidden transcripts*. New Haven, CT: Yale University Press.

Sewell, G., & Wilkinson, B. (1992). 'Someone to watch over me': Surveillance, discipline and the just-in-time labour process. *Sociology*, *26*(2), 271–286.

Simon, B. (2005). The return of panopticism: Supervision, subjection and the new surveillance. *Surveillance and Society*, *3*(3), 1–20.

Singh, S. (1999). *The code book: The science of secrecy from ancient Egypt to quantum cryptography*. Toronto: Random House.

Taleb, N. N. (2004). *Fooled by randomness: The hidden role of chance in life and the markets*. New York, NY: Texere.

Tilly, C. (2005). *Trust and rule*. Cambridge: Cambridge University Press.

Timmons, S. (2003). A failed panopticon: Surveillance and nursing practices via new technology. *New Technology, Work and Employment*, *18*(2), 143–153.

Tversky, A., & Kahneman, D. (1982). Judgement under uncertainty: Heuristics and biases. In: D. Kahneman, P. Slovic & A. Tversky (Eds), *Judgement under uncertainty: Heuristics and biases* (pp. 3–20). Cambridge: Cambridge University Press.

Zetter, K. (2007). Rogue nodes turn to anonymiser's into eavesdropper's paradise. *Wired*, published September 10, 2007, retrieved September 25, 2007, from http://www.wired.com/politics/security/news/2007/09/embassy_hacks