



# Opinion. Privacy is not the antidote to surveillance<sup>\*</sup>

Felix Stalder<sup>1</sup>

We live in a surveillance society<sup>2</sup>. The creation, collection and processing of personal data is nearly a ubiquitous phenomenon. Every time we use a loyalty card at a retailer, our names are correlated with our purchases and entered into giant databases. Every time we pass an electronic toll booth on the highway, every time we use a cell phone or a credit card, our locations are being recorded, analyzed and stored. Every time we go to see a doctor, submit an insurance claim, pay our utility bills, interact with the government, or go online, the picture gleaned from our actions and states grows finer and fatter.

Our physical bodies are being shadowed by an increasingly comprehensive 'data body'. However, this shadow body does more than follow us. It does also precede us. Before we arrive somewhere, we have already been measured and classified. Thus, upon arrival, we're treated according to whatever criteria have been connected to the profile that represents us<sup>3</sup>.

Insurance premiums, for example, can be based on health data that is already available to insurance companies. For our convenience, we are told, the companies already know everything they need to know about us. The problem is that we don't know what they know, and cannot be sure that their information is correct, or become aware of the kinds of decisions that are based upon it. If we are denied insurance coverage, or if our premiums are higher than usual, there is little way of knowing how this decision came about, nor how we can appeal it. After all, receiving a commercial service is a privilege, not a right. If we apply for jobs and do not get them, perhaps it's because of our qualifications, but perhaps it's because we were deemed to be part of a high-risk group for developing health problems, and the company doesn't want to hire employees who might get sick in the future.

This situation makes a lot of people nervous, for good reason. According to every opinion poll taken – at least before the panic regime took over following the terrorist attacks of September 11, 2001 – the vast majority of respondents were "concerned" or "very

---

<sup>\*</sup> An earlier version of this essay, co-authored with Jesse Hirsh, has been published as *Privacy Won't Help Us (Fight Surveillance)* on the nettime mailing list (June 26, 2002).

<sup>1</sup> Department of Sociology, Queens University, Ontario, Canada. Director, Openflows. Website: <http://felix.openflows.org> E-mail: [felix@openflows.org](mailto:felix@openflows.org)

<sup>2</sup> See Lyon (2001); also Norris and Armstrong (1999).

<sup>3</sup> Still the best analysis of this phenomenon is Gandy (1993); for a more theoretical treatment, see Bogard (1996).

concerned" about the misuse of personal data.<sup>4</sup>

Access to large data-sets of personal information is a prerequisite for social control.<sup>5</sup> Those who hold such data have a crucial tool that allows them to influence the behaviour of those whose data is being held. Marketing is an obvious example. The more a seller knows about its prospective customers, the better their needs can be targeted or manufactured. Marketing involves subtle forms of manipulation: creating desires at the right moment, in precisely the right way, so that they can be satisfied by merchants. Similarly, governments want to collect data about their citizens in order to increase the accuracy of their planning, as well as combat fraud and tax evasion. Of course, don't forget the ballooning security establishment, which wants infinite amounts of information about everyone to combat an ever-growing list of enemies.

The cumulative effect of the culling all this information is that "they" know more than ever about "us," while we still know very little about them, including who they are and what they know about us. An increasing number of institutions have the ability to manipulate us, influence our behaviour, and subject us to specialized treatment in a wide range of situations (with various degrees of success, control is never absolute and the claims of the capacities of surveillance technology are often inflated by vendors promoting their products). For instance, when you call your bank and have to wait in line for 25 minutes, you cannot know why. Perhaps it is because you are not a preferred customer, whose call would have been answered immediately, but perhaps it's simply because the system is overloaded. The problem is, you don't know whether this kind of discrimination is taking place, and have no way of fighting against it.

The standard answer to these problems the call for our privacy to be protected. Privacy, though, is a notoriously vague concept. Europeans have developed one of the most stringent approaches where privacy is understood as 'informational self-determination'. This, basically, means that an individual should be able to determine the extent to which data about her or him is being collected in any given context. Following this definition, privacy is a kind of bubble that surrounds each person, and the dimensions of this bubble are determined by one's ability to control who enters it and who doesn't. Privacy is a personal space; space under the exclusive control of the individual. Privacy, in a way, is the informational equivalent to the (bourgeois, if you will) notion of "my home is my castle."

As appealing and seemingly intuitive as this concept is, it plainly doesn't work. Everyone agrees that our privacy has been eroding for a very long time – hence the notion of the "surveillance society" – and there is absolutely no indication that the trend is going to slow down, let alone reverse. Even in the most literal sense, the walls of our castles are being pierced by more and more connections to the outside world. It started with the telephone, the TV and the Internet, but imagine when your fridge begins to communicate with your palm pilot, updating the shopping list as you run out of milk, and perhaps even sending a notice to the grocer for home delivery. Or maybe the stove will alert the fire department

---

<sup>4</sup> For an overview of recent privacy surveys, see: <http://www.privacyexchange.org/iss/surveys/surveys.html>

<sup>5</sup> Probably the most chilling account of this relationship is Black (2002).

because you didn't turn off the hot plate before rushing out one morning.<sup>6</sup> A less futuristic example of this connectivity would be smoke detectors that are connected to alarm response systems. Outside the home, it becomes even more difficult to avoid entering into relationships that produce electronic, personal data. Only the most zealous will opt for standing in line to pay cash at the toll both every day, if they can just breeze through an electronic gate instead.

This problem is made even more complicated by the fact that there are certain cases in which we want "them" to have our data. Complete absence from databanks is neither practical nor desirable. For example, it can be a matter of life and death to have instant access to comprehensive and up-to-date health-related information about the people who are being brought into the emergency room unconscious. This information needs to be too detailed and needs to be updated too often – for example to include all prescription drugs a person is currently using – to be issued on, say, a smartcard held by the individual, hence giving him or her full control over who accesses it.

To make matters worse, with privacy being by definition personal, every single person will have a different notion about what privacy means. Data one person might allow to be collected might be deeply personal for someone else. This makes it very difficult to collectively agree on the legitimate boundaries of the privacy bubble.

From an individual's point of view, making dozens of complex decisions each day about which data collection to consent to and which to refuse, i.e. to actively exercise informational self-determination, is clearly impractical. The cognitive load is too high for all but the most dedicated privacy professionals.

We can see the consequence of this cognitive overload in the well-known paradox that while most people are concerned about privacy, when asked in general terms, in practice most do little to protect it. This dilemma indicates that the “bubble theory” of privacy – based on concepts of individualism and separation – has become unworkable in an environment constituted by a myriad of electronic connections. As many observers has noted, increasingly our societies are organized as networks underpinned by digital information and communication technologies.<sup>7</sup> In a network, however, the characteristics of each node are determined primarily by its connections, rather than its intrinsic properties, hence isolation is an undesirable option. When renting a car anywhere in the world, for example, I do not need a passport – the traditional, stable identifier – but a credit card, which expresses nothing other than my relationship to my bank. A credit card does not say who I am, but whether or not I can be trusted (in a rather specific commercial sense). When important aspects of identity, of what it is to be myself, shift from stable, (quasi) intrinsic properties – nationality – to highly dynamic relationships – credit rating – notions of separation become unworkable. The bubble theory of privacy applies a 19th century conceptual framework to a 21st century problem.<sup>8</sup>

---

<sup>6</sup> For an early vision of intelligent environments, see Mitchell (1995).

<sup>7</sup> Most prominently, Castells (1996).

<sup>8</sup> Elsewhere, I have elaborated on the historical dimension of privacy as connected to the rise and decline of print culture: Stalder (forthcoming).

So rather than fight those connections – some of which are clearly beneficial, some of which are somewhat ambiguous, and some are clearly disconcerting – we have to reconceptualize what these connections do. Rather than seeing them as acts of individual transgression (X has invaded Y's privacy) we have to see them part of a new landscape of social power. Rather than continuing on the defensive, by trying to maintain an ever-weakening illusion of privacy, we have to shift to the offensive and start demanding accountability of those whose power is enhanced by the new connections. In a democracy, political power is, at least ideally, tamed by making the government accountable to those who are governed, not by carving out areas in which the law doesn't apply. It is, in this perspective, perhaps no coincidence that many of the strongest privacy advocates (at least in the US) lean politically towards libertarianism, a movement which includes on its fringe white militias which try to set up zones liberated from the US government.

In our democracies, extensive institutional mechanisms have been put into place to create and maintain accountability, and to punish those who abuse their power. We need to develop and instate similar mechanisms for the handling of personal information – a technique as crucial to power as the ability to exercise physical violence – in order to limit the concentration of power inherent in situations that involve unchecked surveillance. The current notion of privacy, which frames the issue as a personal one, won't help us accomplish that.<sup>9</sup> However, notions of institutionalized accountability will, because they acknowledge surveillance as a structural problem of political power. It's time to update our strategies for resistance and develop approaches adequate to the actual situation rather than sticking to appealing but inadequate ideas that will keep locking us into unsustainable positions.

## References

- Black, E. (2002) *IBM and the Holocaust: The Strategic Alliance between Nazi Germany and America's Most Powerful Corporation*. New York: Three Rivers Press, Random House.
- Bogard, W. (1996) *The Simulation of Surveillance: Hypercontrol in Telematic Societies*, Cambridge, New York: Cambridge University Press.
- Brin, D. (1998) *The Transparent Society. Will Technology Force Us to Choose Between Privacy and Freedom?* Reading, MA: Perseus Books.
- Castells, M. (1996) *The Rise of the Network Society, The Information Age: Economy, Society and Culture (Vol.1)*, Cambridge, MA; Oxford, UK: Blackwell.
- Gandy, O. H. (1993) *The Panoptic Sort. A Political Economy of Personal Information*,

---

<sup>9</sup> One of the few attempts to at least try to think beyond notions of privacy is Brin (1998).

Boulder: Westview Press.

Lyon, D. (2001) *Surveillance Society: Monitoring Everyday Life*, Buckingham, Philadelphia: Open University Press.

Mitchell, W. J. (1995) *City of Bits: Space, Place and the Infobahn*, Cambridge, MA: MIT Press.

Norris, C. and G. Armstrong (1999) *The Maximum Surveillance Society: The Rise of CCTV*. Oxford, UK: Berg.

Stalder, F. (forthcoming): The Failure of Privacy Enhancing Technologies (PETs) and the Voiding of Privacy, *Sociological Research Online*.