

## Are New Technologies the Enemy of Privacy?

Amitai Etzioni

Received: 15 February 2007 / Accepted: 15 April 2007 / Published online: 9 August 2007  
© Springer Science + Business Media B.V. 2007

**Abstract** Privacy is one good among other goods and should be weighed as such. The relationship between technology and privacy is best viewed as an arms race between advancements that diminish privacy and those that better protect it, rather than the semi-Luddite view which sees technology as one-sided development enabling those who seek to invade privacy to overrun those who seek to protect it. The merits or defects of particular technologies are not inherent to the technologies, but rather, depend on how they are used and above all, on how closely their use is monitored and accounted for by the parties involved. In order to reassure the public and to ensure accountability and oversight, a civilian review board should be created to monitor the government's use of surveillance and related technologies. Proper accountability requires multiple layers of oversight, and should not be left solely in the hands of the government.

**Keywords** Luddite imagery · Surveillance society · E-ID

### An Arms Race Versus a Luddite Imagery

The relationship between privacy and technology should be viewed as akin to the relationship between security and technology or prosperity and technology rather than approached from a Luddite perspective. However, much of the literature on privacy follows this second track. It depicts various technological developments, such as electronic databases, computerized searches, and surveillance instruments, as attacks on privacy (for some of the latest writings on technology as eroding privacy, see Whitaker 2000; Garfinkle 2000, and for more reasoned examinations of privacy and technology, see O'Harrow 2005; Solove 2004). Indeed, the more alarmist accounts speak of a 'surveillance society' and the 'death of privacy.' Although these alarmist critics recognize that there is no way to turn back the clock to a pre-digital age, they bemoan the rise of privacy-invading technologies – criticisms similar in tone and terms to the complaints that the Luddites lodged against the development of industrial equipment, from the loom to the steam engine, in the nineteenth century. And like the Luddites, today's critics have, thus, sought to curb these technological advancements if they cannot be eliminated altogether.

Before showing that such critics misunderstand the relationship between privacy and the new technological developments of the digital age, I should reiterate a point that I have spelled out elsewhere: Privacy is

---

A. Etzioni (✉)  
School of International Affairs,  
George Washington University,  
Gelman 703, 2130 H Street,  
NW Washington, DC 20052, USA  
e-mail: etzioni@gwu.edu

merely one good among many others (Etzioni 1999). It always has been and needs to be weighed against other goods, without an a priori assumption that privacy should trump all other considerations. If a child is brought to the emergency room with cigarette burns on his body and X-rays reveal that his arm has been broken twice before, ER attendants will suspect that the child has been subject to abuse. And they are required by law (and by all that is decent) to ask various privacy-violating questions of the child and of those who attend to him, including his parents. Here, the wellbeing of the child trumps both his and his parents' right to privacy. Moreover, historical developments, for instance, the rise of the threat of terrorism, change the relative weight one ought to accord to the privacy of those who seek to enter one's country. More generally, it follows that one ought not to consider every privacy reduction as a social or human loss.

As far as the relationship between technology and privacy is concerned, it is best viewed as an arms race between advancements that diminish privacy and those that better protect it – as opposed to a one-sided development in which those who invade privacy overrun those who seek to protect it. Although several new privacy-diminishing technologies exist or are being created, they are countered by other developments designed to better protect privacy. At any given point in time, new devices of both kinds are created, sometimes altering the balance in favor of privacy and sometimes tipping it in favor of the invaders. Moreover, every new mode of attack tends to invite a quest for a new mode of defense – for example, the way in which new computer viruses invite the formation of new security patches.

True, the balance between privacy-invading and privacy-securing technology is changing all of the time. However, if one compares routine communications today to those of say 1975, one finds a significant net *increase* in privacy, largely due to the development of high-powered encryption. In 1975, the routine communications of an ordinary citizen might have included phone calls (easily 'bugged' or listened to on another extension by a jealous spouse) and letters (readily intercepted and steamed open by the authorities or a jealous lover or employee). Other means of routine communications – postcards and cables – were even less secure and private. In contrast, many of today's routine communications

are sent electronically, secured by high-powered encryption capabilities programmatically built into many computers – capabilities sure to be found on more PCs in the future. As a result, nowadays, when a person sends a routine email via the Internet, it cannot be easily read, even if intercepted, because not only does it travel in divided packets but it also is likely to be encrypted. In short, it is much more difficult today to violate someone's privacy by accessing and reading a routine communication than it was in the pre-digital era.

Turning to non-routine communications, in the past, some senders were willing to engage in extra measures to ensure privacy, such as using a courier or primitive devices like invisible ink and simple code systems, when dealing with highly sensitive or personal communiqués. Today, all of these measures are still available but so is the high-powered encryption discussed above. Granted, it is true that new developments have occurred, enabling those with the knowledge and means to crack such encryption codes and read messages sent from thousands of miles away, say between bin Laden and his mother in Saudi Arabia (Keefe 2005). However, such technologies are highly specialized and costly. In short, when scrutinizing the security of today's communications, one must acknowledge that, in general, the current methods of sending routine and non-routine communications prove much more secure than the avenues used in the past, such as the wire or traditional mail.

The same holds true for the storage of information. Medical and financial records are much more secure in encrypted databases than they ever were in locked cabinets, places where such information has historically been stored. This newfound security also applies to other types of information, as long as it is properly encrypted. The absence of such measures reveals more about the extent to which those involved are not seriously privacy-minded, at least for the data at issue, than it does about a threat from new technologies.

All in all, privacy is challenged but far from dead, and various technological developments will continue to enhance it even as others attack it.

### **Accountability**

Advancements in technology are frequently characterized either as boons or anathemas. The same holds true for those technologies that directly impact

privacy. However, like most technological developments, those concerning the invasion of privacy cannot be easily lumped into simple categories of good or bad per se, although they are often treated in this manner. Instead, their merits or defects depend on how they are used and, above all, on how closely their use is monitored and accounted for by the parties involved. For example, it makes no sense to seek a ban on cameras in public spaces because someone in London used one to violate the privacy of a couple making out in a car (assuming that they had an expectation of privacy in a car parked in a public space in the first place) (Rosen 2001).

To highlight the point, a simple example will serve: Take the case of electronic toll systems, such as the E-ZPass program used in several parts of the USA. Once an individual enrolls in E-ZPass, he receives an electronic device to place in his car. Each time that he travels through a toll, an antenna picks up on the device, and the appropriate amount is deducted from a prepaid toll account. Proponents of such systems see them as a necessity in the face of ever-increasing traffic and argue that they will revolutionize toll collection by minimizing bottlenecks and the need to build additional booths.<sup>1</sup> But privacy advocates, like Jordana Beebe of Privacy Rights Clearinghouse, assert that such toll collections could encroach on individual liberties and worry over how data will be used. Of E-ZPass, Beebe said, "The primary thing to keep in mind with an E-ZPass is basically you're enabling a tracking system."<sup>2</sup>

Yet one should note first of all that, like many technologies cited by civil liberty groups as sources of privacy violations, such as programs enabling credit card orders over the Internet, E-ZPass participation is voluntary. No one is required to use it. However, millions of Americans find they would rather have the convenience of using these technologies than concern themselves unduly with matters of privacy. Indeed, noted privacy expert Alan Westin divides people into three groups. On one end of the spectrum is a minority of the population (25%) that are 'privacy fundamentalists,' deeply concerned about privacy rights, and on the other end is one fifth that are

'privacy unconcerned' (Buskin 2000). The majority (55%) are people that Westin identifies as 'privacy pragmatists,' individuals who tend not to mind personal data collection as long as they feel informed about the solicitor, the possible gains or repercussions of releasing the information, and the safety measures put into place (Buskin 2000). The comments of the chief executive of the Intelligent Transportation Systems, Neal Schuster, suggest that drivers' reasons for choosing E-ZPass prove consistent with Westin's findings: "We do it because of the convenience and we do it because there are laws that protect us."<sup>3</sup>

In any event, the main issue with E-ZPass is not the technology itself but the ways in which it is used – and that use supervised. As with other technologies, E-ZPass can be employed both in ways that most would find unproblematic and quite beneficial and in a manner that many would find very troubling indeed. Suppose, for example, that a car is recorded going through a designated E-ZPass lane. After it is confirmed that the driver prepaid the toll, that record is immediately erased. Few would mind. However, the response would be vastly different if the record in question were filed away and added to other information about us in some comprehensive government dossier in which information about our travels would be kept for years and would be easily accessed by the police, the media, divorce lawyers, and others.

Clearly, for the issue at hand of privacy invasion and protection, the same technology can be used in very different ways. Still, one more crucial step must be undertaken when analyzing technologies involving privacy (and many others) and that is to move beyond assessing each technology on its own merits. The key question is how much accountability and oversight exists for the use to which the technology is put. To return to the example at hand, assume we are told that E-ZPass is used merely in the minimal way described above – information is immediately erased after verification that the toll has been paid, and the information about who traveled when and where is not otherwise available. Still, we might wonder whether these limitations on the use of the information are observed and, if so, who enforces such curbs and how. One major reason we have laws, policing,

<sup>1</sup> "Some concerned about privacy implications of E-Zpass system," *Associated Press*, 21 March 2005. LexisNexis Academic, LexisNexis (28 March 2005).

<sup>2</sup> As quoted in "Some concerned," *Associated Press*.

<sup>3</sup> As quoted in Wickham, S. K., "E-Z Pass: a primer," *Union Leader*, 20 March 2005: A1. LexisNexis Academic, LexisNexis (28 March 2005).

and oversight is that we do not automatically trust the authorities to do what is right.

### How Can Accountability Be Provided?

To some extent, the needed accountability is already built into the government, and it should not be dismissed. For instance, the Inspector General of the Department of Justice issued two highly critical reports of the FBI in 2003. These reports alerted Congress and the public to the FBI's wrongdoings and pressured it to modify its practices. Furthermore, congressional committees have oversight power. And they correctly demanded more specific information about the usage of various powers provided by certain sections of the Patriot Act in an effort to render the uses of the technologies involved, e.g., wiretapping, more legitimate. However, the record shows that, on their own, these committees cannot provide the needed countervailing force to government agencies hell bent on following their own course in the name of national security.

The press, the next line of defense, has been doing a sound job of regularly reporting about a variety of abuses and about programs with absurd designs, leading the government to send many ideas back to the drawing board and to greatly reform aspects of the no-fly lists, the tracking of foreign students, and airport scanning methods, among others.

Many citizens (me included) find these layers of oversight of value but still insufficient. Such people have an inherently healthy distrust of the government and fear that it would conceal information (the way that the CIA kept some detainees off the books), would doctor it, or would refuse to disclose it – even to Congress. To further strengthen oversight for law enforcement authorities and to reassure the public that they are not running amok, we need a civilian review board. It would be composed of the kind of people who served on the 9/11 Commission: bipartisan, highly respected by the public, able to work together, not in the running for public office, and patriotic. These individuals would need the proper level of security clearance to review detailed records to ensure that nobody is pulling the wool over their eyes. The board would issue regular reports about its generalized findings without revealing specifics about sources and methods. Such oversight would allow one and

all to determine whether, in most cases, the search of databases, delayed disclosure, and other new security measures have been employed legitimately and used for good purposes or whether the opposite is the case. Such reports should lead to internal reforms in government agencies, as they will have to expect future rounds of similar audits.<sup>4</sup>

### Reliable E-ID

To close, I point to a new technological development that would greatly enhance privacy. New technologies are now being developed and introduced that would allow people to present proof of their identity when communicating via the Internet, much like presenting a passport when crossing national borders. Sometimes referred to as 'digital certificates,' such E-IDs can be provided through a 'certificate authority' or CA, such as GeoTrust or VeriSign. Once established, these digital certificates consist of a variety of information that enables those on the other end of a business transaction to confirm that an individual is who he says he is. The electronic postmark (EPM) extension launched by the US Post Office in partnership with Microsoft and AuthentiDate in October of 2003 is just one example of a technological development that seeks to provide reliable E-IDs.<sup>5</sup> Overall, such E-IDs make it much more difficult for unauthorized persons to gain access to a variety of information, and they will help to minimize identity theft.

<sup>4</sup> A blueprint for such a civilian review board was sketched with the passage into law of the Intelligence Reform and Terrorism Prevention Act (Public Law 108-458) on December 17, 2004. Subtitle F, Section 1061 of this Act called for the creation of a Privacy and Civil Liberties Oversight Board. However, one should note that some critics feel that the Board as approved lacks the necessary independence and power to be an effective mechanism of oversight. Thus, Representatives Tom Udall and Carolyn Maloney brought forward a new bill in March 2005, "The Protection of Civil Liberties Act," aimed at restructuring this Board. The legislation is currently being reviewed by various committees. For additional information, please see Public Law 108-458, 108th Cong., 2d sess. (17 December, 2004), *Intelligence Reform and Terrorism Prevention Act of 2004*, 48-52; Press Office, "Udall Renews Call for 'Independent' Civil Liberties Board," Congressman Tom Udall. <<http://www.tomudall.house.gov/issues2.cfm?id=10264>> (3 May, 2005).

<sup>5</sup> Microsoft Office Online, "Sign and send business documents electronically with USPS electronic postmarks," Microsoft. <<http://office.microsoft.com/enus/assistance/HA010971711033.aspx>> (29 April 2005).

The technology behind E-IDs is complex and in flux, and it is not my purpose in this paper to enter into an explanation of its intricacies, especially considering the many different options offered by various vendors. I simply wish to outline the basic concepts of E-IDs as a means by which to provide another example of how some advancements in technology *are helping to safeguard privacy as others infringe upon it*.<sup>6</sup>

## Conclusion

In conclusion, privacy is under attack by new technologies, but it is also benefiting from new technologies. Those concerned about privacy should work to improve the regulations controlling the use of these technologies rather than adopt a semi-Luddite position, hoping these technologies will go away or be suppressed. How carefully the use of various technologies is monitored is, as a rule, more important than the capabilities of the technologies themselves. Proper accountability requires multiple layers of oversight.

And for that accountability to be fully effective in limiting abuse and building public trust, it cannot be left solely in the hands of the government.

## References

- Buskin, J. (2000). "Choice and Trust," *Wall Street Journal*, (April 17), R34.
- Etzioni, A. (1999). *The Limits of Privacy*. New York: Basic Books.
- Garfinkle, S. (2000). *Database Nation: The Death of Privacy in the 21st Century*. New York: O'Reilly.
- Keefe, P. R. (2005). *Chatter: Dispatches from the Secret World of Global Eavesdropping*. New York: Random House.
- O'Harrow, R. (2005). *No Place To Hide: Behind the Scenes of Our Emerging Surveillance Society*. New York: Free Press.
- Rosen, J. (2001). "A Watchful State," *New York Times Magazine*, (October 7).
- Solove, D. J. (2004). *The Digital Person: Technology and Privacy in the Information Age*. New York: New York University Press.
- Whitaker, R. (2000). *The End of Privacy: How Total Surveillance is Becoming a Reality*. New York: New Press.

<sup>6</sup> For more detailed descriptions of the technologies involved in electronic identities, please see the following: Bryan-Low, C., "Identity Thieves Organize," *Wall Street Journal*, 7 April 2005: B1. <[http://online.wsj.com/article\\_print/0,,SB111282706284700137,00.html](http://online.wsj.com/article_print/0,,SB111282706284700137,00.html)> (15 April 2005); Caffrey, A. "USPS Wants to Deliver Fairness to Mutual Funds USPS Wants to Deliver Fairness to Trades," *Boston Globe*, 17 May 2004: C1. *LexisNexis Academic*, LexisNexis (16 April 2005); Glassman, M., "The Electronic Verification Is in the Mail," *New York Times*, 22 January 2004: G3. *LexisNexis Academic*, LexisNexis (16 April 2005); Guth, R. A., "Microsoft Tests Software To Fight Identity Theft on Web," *Wall Street Journal*, 28 March, 2005: B1. <[http://online.wsj.com/article\\_print/0,,SB11196644239490480,,00.html](http://online.wsj.com/article_print/0,,SB11196644239490480,,00.html)> (16 April 2005); Harlin, K., "AuthentiDate poised to make its mark online," *Times Union* (Albany, NY), 7 August 2002: E1. *LexisNexis Academic*, LexisNexis (16 April 2005); Kingson, J. A., "Banks Test ID Device for Online Security," *New York Times*, 24 December 2004: C1. *LexisNexis Academic*, LexisNexis (12 April 2005); Microsoft, "Sign and send"; United States Postal Service Media Relations, "Postal Service EPM Digitally Protects Microsoft® Documents," United States Postal Service. <[http://www.usps.com/communications/news/press/2003/pr03\\_076.pdf](http://www.usps.com/communications/news/press/2003/pr03_076.pdf)> (16 April 2005).