

N. Katherine Hayles

Literature Program, Duke University, Durham NC, USA.

In February 2009 the House of Lords Constitutional Committee in the United Kingdom published the report *Surveillance: Citizens and the State*. Some have hailed this as a landmark document. The following is one of four commentaries that the editors of *Surveillance & Society* solicited in response to the report.

In depth, breadth, and even-handedness, *Surveillance: Citizens and the State*, Volume 1 of a Report to the Select Committee on the Constitution of the House of Lords (hereafter the *Report*) is an impressive document. There is, however, an absence at its core that I want to address. Surveillance technologies such as CCTV cameras, RFID tags, the National DNA Database and corporate databases can be properly assessed only if the countervailing right of privacy is strongly articulated and broadly understood. This the document fails to do, suggesting in its preliminary remarks that “the loss of privacy in some cases may be harmless and may be offset by the benefits of surveillance and data collection” (15), noting that “prior to the enactment of the Human Rights Acts 1998 (HRA), there was no established right to privacy in UK law.” Rather, the appeal was to the European Court of Human Rights. Only in 1998 with the HRA did Article 8 become part of domestic law, so that “a general right to respect for private and family life . . . was established in the UK” (30). This assessment notwithstanding, the report falls back on US Supreme Court Justice Louis Brandeis’s 1890 definition of privacy, “the right to be let alone,” supplementing that with the 1990 Calcutt Committee on Privacy and Related Matters: “The right of the individual to be protected against intrusion into his personal life or affairs, or those of his family, by direct physical means or by publication of information” (31). There are a number of surveillance techniques—collection and retention of purchasing behavior in corporate databases, for example—that this definition does not cover. In addition, it does not provide a strong rationale for why privacy should be protected as a social good.

Privacy is essential because it provides a space for resistance to the hegemonic power of states and corporations. Michel Foucault’s work on archaeologies of knowledge has taught us to recognize the structures through which such power is disseminated and enforced. The great lesson to be learned from his work is the inescapability of power’s effects, permeating every aspect of social relations, conduct, knowledge structures, and institutions. Yet if there is a weak point in Foucault’s work, it is the inability to account for change. How and why does social change come about? Privacy, I want to suggest, is a crucial mechanism fostering change to the extent that it acts as a blockage to the flow of state and corporate power. To be sure, the barriers created by privacy are never entirely impermeable or completely effective. Nevertheless, in best case scenarios they hamper hegemonic influence so that spaces are opened up in which people can think their own thoughts, including subversive or revolutionary ideas, and most important for our purposes here, innovative and creative ones.

Hayes, N. Katherine. 2009. Waking up to the Surveillance Society. *Surveillance & Society*, 6(3): 313-316.

<http://www.surveillance-and-society.org> | ISSN: 1477-7487

© The author(s), 2009 | Licensed to the Surveillance Studies Network under a [Creative Commons Attribution Non-Commercial No Derivatives license](https://creativecommons.org/licenses/by-nc-nd/4.0/).

It is not merely coincidental that when writers want to suggest the possibility of resistance to state hegemony, they typically begin with the discovery of an unregulated space, a *private* space: the room that the lovers discover in Orwell's *Nineteen Eighty-Four*; the storeroom of the underground eatery where Sonmi-451 and her colleague discover books in David Mitchell's *Cloud Atlas: A Novel*; the mysterious hallway that opens up in the suburban house in Mark Danielewski's *House of Leaves*. These are spaces in which unauthorized, rebellious, and even dangerous thoughts can be entertained; they are also catalysts to discovery, innovation, and potential change. Privacy in this view is not merely an individual right but a positive social good, for it is the cradle from which can grow the resistance, creativity and innovation essential for the renewal of a society. That it necessarily can also foster rebellion, deviancy and crime does not negate its positive potential; this is the price we pay for diversities of thought, varieties of practices, and differences of views. Without privacy, the coercive force of hegemonic power to control not only behavior but the innermost thoughts of citizens becomes absolute.

Only when the essential contributions of privacy to a healthy society are understood can we properly assess the balance between the social needs for surveillance and the rights of citizens for privacy in their lives. Privacy means more than just "going about our business undisturbed," as one respondent to the Select Committee on the Constitution put it. It means the *presumption of freedom* from having our affairs overlooked by others, absent compelling reasons to the contrary; it means *having access to data* that has been collected on us by interested parties; it means *having control over* how data about our private lives is used and by whom; it means *the right to establish boundaries between public and private spaces* that are lawfully enforced and respected by everyone, including functionaries at every level of government, from town councils to national agencies, and at every level of corporate activity, from local stores to transnational databases.

Given these strong arguments and clear guidelines for the protection of privacy, how might we assess the different kinds and areas of surveillance detailed in the *Report*? The three surveillance technologies on which I will focus are Radio Frequency Identification technology (RFID), closed circuit TV, and the National DNA Database (NDNAD). RFID redefines surveillance (see: Hayles 2009), because unlike other surveillance modes that require visible devices such as CCTV cameras, they operate ubiquitously and invisibly in the environment. RFID tags come in two varieties, active and passive. Passive tags report back a 10-digit unique identification code when pinged by a RFID reading device; active tags typically carry more information and have their own power source, capable of broadcasting signals up to a mile. Since RFID does not require a clear line of sight to work, RFID tags can be embedded in packaging, sewn into clothing labels, and hidden in shoes and purses, thereby identifying these items by their unique ID numbers (in contrast to UPC, which merely provides generic identification). Embedded into passports, RFID can contain biometric and personal data, including retinal scans and fingerprints. Linked with back-end databases containing information gathered through "loyalty cards" that give a discount in exchange for relinquishing personal data, RFID numbers can be correlated with a wide variety of consumer information, including names, social security numbers, credit card numbers, buying habits, etc. The results are fine-grained analyses of consumer behavior on a scale and depth never before possible. Note that these results are *not* anonymized but specific to individuals. RFID instantiates the transition that Gilles Deleuze foresaw from a carceral system of discipline, in which individuals are controlled by physically enclosing them in schools, barracks, prisons, etc., to a control society where citizens are disciplined through a real-time monitoring of their behaviors as they move with apparent freedom through space.

Although RFID tags and related databases can be used to control populations directly, for example through RFID-embedded passports, more typical are their uses in marketing products. These uses are not without dangers. Data repositories present an ever-present risk of being hacked into and having data stolen. The more information they contain, and the more databases are interlinked with one another, the more vulnerable we all are to having our personal information compromised. Moreover, insofar as RFID allows commercial interests to construct detailed profiles of our activities, they undermine the right to privacy, eroding the barrier between public and private spheres. Commonsense remedies can curb these abuses. RFID tags can be manufactured so that a tear-off tab can be removed when a garment or other

object is purchased, making it impossible to track items after a consumer owns them. The presence of RFID tags can be identified with an easily visible symbol, so that citizens know when and where the technology is being employed. Laws can be passed regulating the extent to which RFID tags can be used to identify people and track their movements without informed consent, thus preventing such practice as having schoolchildren wear RFID bracelets (now common in Japan). Many other kinds of legal and social protections are possible, but the first step is increasing public awareness. Although RFID is mentioned in the *Report*, its full potential as a surveillance technology is under-reported in that document.

CCTV receives better coverage. The shocking revelation here is how extensive CCTV has become in the UK—an estimated 4 million cameras are on the lookout—and how many loopholes there are in present regulatory and legal safeguards. Some of the worst abuses occur at the local level, where citizens are surveilled for such minor offenses as not cleaning up after one's dog. While there continues to be popular support in the UK for CCTV as a deterrent to crime, the regulatory structure appears to be in disarray. For example, there is apparently no regulation governing the use of CCTV if no recording is made of the surveillance. The *Report* contains several important recommendations in this regard, including the revision of the Regulation of Investigatory Powers Act 2000 (RIPA) to require judicial oversight for targeted surveillance, and a reconsideration of whether local authorities should be given RIPA powers.

DNA is arguably one of the most intrusive of surveillance technologies, in that DNA is considered a unique identifier and can be brought to bear on tiny samples long after the event. The safeguards should accordingly be strict. Quite the contrary is the case in the UK, however. Surveillance in the form of the National DNA Database (NDNAD) includes taking DNA samples from anyone arrested for a “recordable offense,” whether or not that person is later found guilty or indeed even charged with a crime. In addition, DNA samples from witnesses are also entered into the NDNAD and not expunged after the judicial proceedings are over. These practices have resulted in a disproportionate percentage of the population being entered into the NDNAD—a shocking 7.39%, much higher than any other European country and fifteen times higher than the .5% of the US population in the FBI's “CODIS” database. Moreover, the tendency of law enforcement officers toward racial profiling means that certain populations are disproportionately likely to be arrested without being charged, especially young black men, who are consequently present in the NDNAD far in excess of their numbers in the population.

As the *Report* drily insinuates, there is a good deal of official hypocrisy in this regard. The National Policing Improvement Agency (NPIA), the custodian organization of the DNA database, argued that “inclusion in the DNA Database does not signify a criminal record and there is no personal cost or material disadvantage of the individual simply by being in it” (45). Such a position, of course, would trample on the right of privacy and jeopardize the relation of citizens to the state, making everyone in the database an automatic suspect to be checked against any crime that the authorities saw fit to prosecute. Following the party line, Tony McNulty MP (at the time of the *Report* the Minister for Security, Counterterrorism, Crime and Policing at the Home Office) disingenuously testified that the NDNAD is “not an information source for all the naughty and potentially nasty people in the country. . . It is purely an informational and investigatory device for the police” (45-46). If indeed there is nothing prejudicial about being in the NDNAD, then there should be nothing wrong with solving the inequities by having everyone entered into it. But this, of course, would truly lead to an Orwellian society, a prospect that no one even marginally concerned with civil liberties would endorse. The *Report* uses such reasoning to show obliquely the hypocrisy of McNulty and others, saying that the Committee finds itself “puzzled” by McNulty's opposition to a universal database because of “practical civil liberties” and “potentially legal concerns” (46).

Along with recommendations that aim to purge non-offenders from the NDNAD and increase oversight, one of the important reforms that the *Report* recommends is strengthening the role of the Information Commissioner, who oversees the Data Protection Act 1998 (DPA) and the Privacy and Electronic Communications Regulations, in addition to the Freedom of Information Act 2000. The Information Commissioner therefore should have regulatory oversight over commercial databases, including

determining whether security safeguards are adequate and preventing many databases from being linked together, crucial issues for the protection of privacy. However, under present law, the Information Commissioner can only inspect data gathering and storage procedures if the company agrees to his inspection, which is rather like asking the fox for permission to check if the chickens are OK. In recommending a stronger role for the Information Commissioner, the *Report* extends its concerns beyond governmental surveillance into the corporate realm, a development very much needed.

The *Report's* significance goes well beyond the particularities of surveillance in the UK, revealing as they are in their own right. In surveying the multiple sites at which surveillance can be carried out, listing the diverse technologies contributing to a surveillance society, and interrogating the legal and regulatory structures charged with controlling them, the *Report* provides a comprehensive and detailed picture of how a society famed for its civil liberties can nevertheless “sleepwalk into” a surveillance society, as the *Report* notes on a number of occasions. Supplemented with a stronger case for the right of privacy as a pre-eminent social good, it provides a blueprint of concerns and issues that should serve as a wake-up call to everyone.

References

- Danielewski, Mark. 2000. *House of Leaves*. New York: Pantheon.
- Deleuze, Gilles. 1992. Postscript on the Societies of Control, *October* 59: 3-7
- Foucault, Michel. 1995. *Discipline and Punish: The Birth of the Prison*. New York: Vintage.
- Hayles, N. Katherine. 2009. RFID: Human Agency and Meaning in Information-Intensive Environments, *Theory, Culture, and Society* 26(2/3): 1-26
- Mitchell, David. 2004. *Cloud Atlas: A Novel*. New York: Random House.
- Orwell, George. 2003. *Nineteen Eighty-Four*. New York: Plume.