

Oscar H. Gandy Jr.

Emeritus Professor of Communication, University of Pennsylvania, USA, <mailto:ogandy@asc.upenn.edu>

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 February 2009, staff at the US Federal Trade Commission (FTC) issued a special report on behavioral advertising (FTC Staff). Consistent with the ruling ideology that has shaped the FTC's efforts over the years, the report continued to advocate self-regulation as the best way to protect the interests of consumers despite mounting evidence to the contrary. In a separate comment, Commissioner Pamela Harbour did take issue with some aspects of the staff report. She expressed serious doubts about the assumption that consumers were fully aware of the kinds of "bargains" they are assumed to have entered into when they visit different sites around the web (Jones Harbour 2009). Commissioner Harbour also concluded that technological solutions like opt-out cookies were an inadequate response to the problem of informed choice in a rapidly evolving network environment. Finally, she challenged the complacency with which the FTC's staff treated distinctions among the different types of information that should be subject to some form of self-regulatory attention on the basis of its uncertain status as "personally identifiable."

I suppose that there is some small comfort to be derived from the fact that at least one member of the government agency with primary responsibility for protecting privacy in the US is aware of some of the ways in which private business activity continues to degrade the value of privacy and confuse its meaning. But this kind of partial dissent is a far cry from the kind of response that we might have received had the policy recommendations made previously by the National Research Council Committee on Privacy in the Information Age actually transformed the laws of the land (Waldo, Lin and Miller 2007).

As a member of the National Research Council committee, I was pleased that we had concluded that the "overall impact of advancing technology including IT has been to compromise privacy" (ibid: 312), in addition to noting "self-regulation is limited as a method for ensuring privacy" (ibid: 328). It was also important that we recommended that the principles of fair information practices should be extended to private sector organizations that collect and use personal information at the same time that we recommended that a privacy commissioner, or a standing privacy commission should be established. However, the fact is that our recommendations, as "radical" as they may have seemed at the time, still limited the scope and power of this commissioner to making ongoing "assessments of privacy developments" (ibid: 341). Had our recommendations been successful in this regard, the long-term impact of such an office would have been minimal at best.

Despite the fact that the Information Commissioner (IC) in the UK had already been assigned considerably more power and authority under the Data Protection Act of 1998 than we had proposed for the US, it appears that there may still be more to come. The recent report on surveillance from the House of Lords conveyed the clear sense that an extension of responsibility and an enhancement of power and resources not only were in order, but that such a structural response had already gathered considerable political support. Citing the large number of witnesses who “called for an expansion in the role of the Commissioner and for his powers and resources to be increased,” the Select Committee’s overall impression was that there was “a pressing need to strengthen his regulatory hand” (House of Lords 2009: 54).

The Commissioner apparently agreed with these assessments, indicating in his own testimony that the efforts of his office could be improved in several ways, including a requirement that privacy-intensive organizations consult with his office prior to introducing “significant new developments.” In addition to the “increased audit and inspection powers” that would include private, as well as public sector organizations within the broad scope of his mission, the Commissioner also sought “effective penalties for serious disregard for the requirements of the data protection principles” (ibid). Supporters of an expanded role for the IC suggested that the public interest would be well served if the Commissioner were not only allowed to, but would have a “statutory obligation” to warn Parliament about significant threats to privacy that were apparent in legislative or regulatory proposals.

Of course, it remains to be seen whether the expansion of the IC’s powers that had been incorporated in the Criminal Justice and Immigration Act of 2008 will be matched with the financial resources that will be required to move beyond the promotion of public awareness to the actual enforcement of data protection. Still, there is far more reason to be hopeful in the case of the UK than in the US because of a critical difference in the roles that the FTC and the IC have been assigned.

The report on surveillance makes it clear that the Information Commissioner’s Office (ICO) has a sufficiently strong commitment to privacy. The ICO’s expressions of concern about the threats to privacy associated with an expansion of surveillance would lead most observers to characterize the function and orientation of that office as one of advocacy. The FTC, on the other hand, appears to treat sophisticated techniques of marketplace surveillance and consumer segmentation as an enhancement of business capacity and a spur to the efficiency of markets, while the protection of privacy is generally seen as a burden that has to be minimized. The role of the FTC appears to be similar to that of the “Chief Privacy Officers” that are becoming routine fixtures within privacy-intensive firms in the US. Their function is to protect the organizations against liability and other risks associated with their acquiring and using personal information, not to protect consumers, or defend privacy.

It should be noted that when the members of the Select Committee visited Canada as part of their inquiry they included discussions with numerous representatives from several Canadian Information and Privacy Offices, as well as with representatives from the Department of Justice, the Public Prosecution Service, and the Supreme Court of Canada. Additional discussions were held with scholars and experts from public interest organizations. The Committee’s visit to the United States did include a visit at the Federal Trade Commission, but it probably only reinforced the impression that the FTC was not seriously engaged with the problem of surveillance. Indeed, for the FTC, the absence of any record of “problems or complaints” under the “safe harbor” arrangements the US developed in response to the EU Data Protection Directive “was taken to be an indication of adequacy” (ibid: 129). Discussions with members of the public interest community in the US, however, were far less sanguine about the adequacy of the government’s response to the challenge of “ubiquitous surveillance.”

Just because developments in the UK’s ICO have advanced so far beyond those in the US does not mean that there is not still important work to be done. The report on surveillance made it quite clear that the standard of privacy protection that had been achieved in the UK was actually quite some distance behind levels attained in Germany and in Canada. For some time Germany has been a leader in the European

Union (EU), especially with regard to support for “informational self-determination” and actions by citizen-consumers seeking to preserve the meaning and value of autonomous action. Like Germany, Canada not only has a national office devoted to protecting privacy, but individual provinces and territories have their own privacy commissioners.

However, as the UK surveillance report suggests, there is considerably more work to be done in order to ensure that the protections that have been established are not degraded by the normalization of new forms of surveillance, or more critically, by their expanded use in support of discrimination in markets and in the public sphere. First it should be noted that even though the UK report is really quite advanced in terms of its understanding and appreciation of the meaning of surveillance as a social practice, it has not paid very much attention to the role that surveillance plays in producing cumulative disadvantage within society (Gandy Jr. 2006).

In the section on “data mining and profiling,” the report limits its discussion to decisions being made within public service agencies that “may arguably lead to discrimination by singling out individuals or social groups for adverse treatment on the basis of incorrect or misleading assumptions” (House of Lords 2009: 14). Later, in the section specifically focused on “surveillance and discrimination,” there are signs that the IC does appreciate some of the ways in which profiling may lead to “greater stigmatization, more discrimination, more social exclusion and a society of greater suspicion where trust is reduced” (ibid: 28).

Sensitivity with regard to how this group-focused discrimination is likely to have a racial character was also emphasized in discussions of developments in the use of genetic profiles. However, discussion of the consequences that are likely to flow from the private sector’s use of transaction-generated information (TGI) were barely noted at all. The only evidence of any sustained attention to these matters emerged just briefly in the Appendix, where a roundtable discussion at the University of Ottawa touched on public opinion and “reasonable expectations of privacy.” Apparently, public awareness of surveillance and data protection issues had improved in Canada to the extent that some people were aware that “data could sometimes be used in ways which could result in discrimination against certain types of people” (ibid: 119).

Although concerns about discrimination were expressed rather sparingly in the House of Lords report, they were completely absent from the FTC staff report on “protecting consumers in the next tech-ade” (FTC Staff 2008), and the more recent staff report on behavioral advertising (FTC Staff 2009). Both reports included frequent references to the threats to consumer privacy associated with the failure of data gatherers to secure the information, and to protect against “misuse.” The problem, of course, is that the use of TGI as an aid to economic discrimination is not considered a misuse, but a legitimate business practice (Gandy Jr. 1996).

Although it is important that privacy advocates, including information and privacy commissioners, should make every effort to inform the public about how TGI is being used to limit their ability to make informed choices within markets and within the public sphere, it is also important for us to be aware of how estimates and representations of public opinion have been used strategically to distort the true nature of growing public concerns about this kind of discrimination (Gandy Jr. 2003).

Of course, before information and privacy commissioners can inform the public about the ways in which TGI leads to invidious distinctions, unjust discrimination, and cumulative disadvantage, they need to learn a great deal more about this process themselves. Recently, warnings about the nature of risks associated with the capture and use of TGI have begun to emerge from a rather unexpected source deep within the surveillance infrastructure. Gregory Conti, a computer specialist teaching at the US Military Academy at West Point, has begun to issue warnings about the kinds of personal and systemic risks we should associate with the use of Google and other Internet search resources (Conti 2006).

Conti's contribution begins with a reminder that "every interaction we have with an information service provider discloses some information." The fact that organizations like Google are able to capture, store, and search for patterns in the data generated from search, email, news reading, and a host of other services offered by its subsidiaries, clients, and partners means that these organizations have the ability to develop "content and behavior-based fingerprints" of the sort that privacy advocates have barely begun to imagine (see Solove 2004, O'Harrow 2005). For Conti, and many other critical observers, the concern is that the collection and use of TGI, including that generated as a byproduct of searches, ensures greater accuracy or precision in the identification and classification of individuals on the basis of their behavior. The data being amassed and processed through data mining facilitates the association of computer users' digital activities with their "real world personas." It is, as David Phillips (2004) suggests, relatively easy for a person to move from anonymity to reliable indexical identification in an era of massive routine data capture and analysis.

Conti sets aside mainstream and traditional concern about the kinds of errors that might be made in compiling individual profiles. He is far more concerned about the sorts of risks we might face if Google's corporate motto and underlying philosophy of "don't be evil" begins to depart from the traditional meanings of that motto (Marrone 2009). It is not even necessary for Google or the managers of its subsidiaries to depart from their public stance. The fact that these massive databases are readily available for a variety of questionable uses, such as generating detailed maps of the homes of individuals making political contributions,¹ or facilitating government determinations of the nature of pornographic sites on the web² means that the zone of reasonable expectations of privacy will continue to shrink at a rapidly accelerating rate.

In Conti's view, it is not so much that they might "get it wrong" that matters. It is the fact that these profilers make use of data and techniques that "provide unprecedented clarity on virtually all aspects of our personal and professional lives." From a policy perspective what matters is the ability of people to limit the amount of TGI that can be captured, and then to limit the uses to which it can be put.

Of course, we are going to have to look beyond the UK's ICO, or the recent surveillance report for guidance on how to address a fundamental problem with policy frameworks that are derived from a traditional focus on individually identifiable information. It is of course true that people suffer the consequences of discrimination as individuals. But the truth is that people are not victimized primarily on the basis of their identification as unique individuals; they are discriminated against on the basis of their identification as members of groups. Increasingly these new groups are not the familiar constructions based on race, gender and class. These groups are the products of multivariate statistical analysis and idiosyncratic naming strategies that more clearly reflect the business plans of the users of the data, than they reflect the self-awareness of the people who have been defined. As a result, these synthetic "groups" have no political identity, and little possibility of organizing as an interest group that might pursue its interests within the public sphere.

As Phillips suggests "should legislators wish to create a more fundamentally equitable information regime, they should consider operationalizing data laws not in terms of information that identifies individuals, but instead information that is produced by or pertains to individuals, whether those individuals are identifiable or not" (Phillips 2004: 704). The surveillance report suggests that the ICO is moving in the right direction. We can only hope that the new administration in the US will have the good sense to follow along.

¹ A website used Google maps to identify bay area contributors to the campaign to limit same sex marriages in California (See Stone 2009).

² In the case of *Gonzales v. Google, Inc.*, No. CV 06-8006MISC JW (Mar. 17, 2006), the US government sought access to search records to be used in a continuing struggle over online access to pornographic materials. Google resisted, while Yahoo, MSN and others readily complied with the overly-broad request for TGI.

References

- Conti, Gregory. 2006. "Considering Google harmful." Conference paper. New Security Paradigms Workshop, Schloss Dagstuhl, Germany. September.
- FTC Staff 2008. "Protecting consumers in the next tech-ade: A report by the staff of the Federal Trade Commission. Report. Washington, DC: Federal Trade Commission. March
- FTC Staff 2009. "Self-regulatory principles for online behavioral advertising." Report. Washington, DC: Federal Trade Commission. February
- Gandy, Jr., Oscar H. 2006. "Quixotics unite! Engaging the pragmatists on rational discrimination," pp. 318-336 in *Theorizing Surveillance: The Panopticon and Beyond*, edited by D. Lyon. Portland, Ore: Willan Publishing.
- Gandy, Jr., Oscar H. 2003. "Public opinion surveys and the formation of privacy policy." *Journal of Social Issues* 59:283-299.
- Gandy, Jr., Oscar H. 1996. "Legitimate business interest: No end in sight? An inquiry into the status of privacy in cyberspace." *University of Chicago Legal Forum*, 1996: 77-137.
- Jones Harbour, Pamela. 2009. Concurring statement regarding staff report, "self-regulatory principles for online behavioral advertising." Washington, DC: Federal Trade Commission, February.
- House of Lords. 2009. *Surveillance: Citizens and the State*. Vol. 1: Report. Select Committee on the Constitution. London: The Stationery Office Limited. February.
- Marrone, Matt Marrone. 2009. "Is Google evil?" *New York Daily News*. Online. March 13, 2009. http://www.nydailynews.com/tech_guide/2009/03/13/2009-03-13_is_google_evil.html?
- O'Harrow, Robert O'Harrow. 2005. *No Place to Hide*. New York: Free Press.
- Philips, David. 2004. "Privacy policy and PETs." *New Media & Society* 6:691-706.
- Solove, Daniel. 2004. *The Digital Person: Technology and Privacy in the Information Age*. New York: New York University Press.
- Stone, Brad. 2009 "Prop 8 donor web site shows disclosure law is 2-edged sword." *New York Times Online*. February 8, 2009. <http://www.nytimes.com/2009/02/08/business/08stream.html?>
- Waldo, James, Herbert Lin and Lynette Millett (Eds.). 2007. *Engaging Privacy and Information Technology in a Digital Age*. Washington, DC: National Academies Press.