ROBERT GELLMAN
Privacy and Information Policy Consultant **202-543-7923**
419 Fifth Street SE **bob@bobgellman.com**
Washington, DC 20003 **www.bobgellman.com**

The Privacy Advocates: Resisting the Spread of Surveillance
By Colin J. Bennett
MIT Press 2008

Review by Robert Gellman
November 4, 2008
Version 1.0

Who are the privacy advocates and how do they function? Colin Bennett, a professor of political science at the University of Victoria, British Columbia, Canada, sets out to answer this question in his new book, The Privacy Advocates. Every privacy advocate, technology company, marketer, government agency, and any one else who cares about privacy or doesn't want to be the subject of a privacy campaign will benefit from reading this book.

Much privacy scholarship explores what privacy is, why anyone should care, and what, if anything, should be done to respond to activities and technologies that diminish privacy. Colin Bennett pays respects to this "vast literature" and then goes where no one has gone before. He seeks to explain privacy advocates, their organizations and operations, why they succeed or fail, and the future of the privacy movement.

Bennett's credentials are impeccable. He is himself is a major contributor to privacy literature. His 1992 Regulating Privacy is among the best and most readable of the academic privacy books. It offers an examination of the international policy convergence that developed in the last part of the twentieth century around fair information practices. Bennett also teamed up with Charles Raab in The Governance of Privacy.

Bennett's qualifications also include being a privacy advocate himself, something disclosed immediately in the introduction. The study is nevertheless free of any apparent bias. Disappointingly from a gossip perspective, it is also free of attempts to settle old scores. Bennett used his insider's knowledge to obtain direct and unparalleled access to many members of the privacy community (including this reviewer, who admits to being part of the privacy community while denying being a privacy advocate).

Another noteworthy qualification is that Bennett is Canadian, which gives him an outsider's perspective of the United States. The book usefully covers privacy advocates in Canada and in Europe as well as the U.S... Most privacy advocates outside the U.S. operate in jurisdictions that have privacy agencies. Bennett speculates that the presence of a government privacy agency has the unintended effect of crowding the policy space and leaving less room for independent privacy advocacy. I doubt that would be the case here, but I would love to find out. See my article: *A Better Way to Approach Privacy Policy in the United States: Establish a Non-Regulatory Privacy Protection Board*, 54 Hastings Law Journal 1183 (2003), http://bobgellman.com/rg-docs/rg-hastings-2003.pdf.

Bennett does better at describing privacy advocates than defining them because "there are no easy generalizations about what makes and motivates privacy advocates." Like a skilled chef with a knife, he slices and dices privacy advocacy this way and that to produce a finely detailed examination of groups, actors, strategies, and networks. He finds several different flavors of privacy groups: privacy-centric, civil liberties, human rights, consumer protection, digital rights, and single issue. For privacy actors, the flavors are activist, researcher, consultant, technologist, journalist, and artist (!). His list of strategies considers information politics, symbolic politics, accountability politics, and leverage politics. Every type is illustrated with a real example. These descriptions are the heart of the book, offering both history and analysis.

One of the most interesting chapters provides a detailed review of "cases that reach higher levels of public and political consciousness." The "paradigmatic" cases include census battles, ID card protests, marketing activities, the Clipper Chip, and more. For those who lived through these campaigns, the review is a welcome revisit of past glories. For newbies, it is basic history and education.

People on either end of a privacy campaign will find great value in the chapter's observations about the conditions for success of a privacy campaign. One of Bennett's conclusions is that getting the facts wrong can have destructive consequences for a privacy campaign, and he is surely right on this point. He also emphasizes the need for advocates to work in a coalition if a campaign is to succeed. Elsewhere in the book, Bennett discusses some failed privacy campaigns as well as the counter tactics that caused them to fail. The book would have been better if it included more analysis of advocacy failures.

> ➔ At the conclusion of this review, I offer my own short case study of an "accidental" privacy campaign in the United States that had significant long-term consequences. It is a story that many never knew or have forgotten, and it is worth memorializing somewhere.

Bennett uses his political science skills to try to place privacy advocates within the categories that political scientists have developed for analyzing movements, public interest groups, and transnational activism. For example, one cited authority describes a *social movement organization* as segmentary, polycentric, and networked. On this scale, Bennett finds the privacy advocacy network to be "not unlike" other social movements. But not exactly. The differences are likely to be of more interest to political science readers than to privacy readers. Political science jargon generally leaves me cold. In any event, privacy advocacy never seems to fit neatly in any existing category. Privacy is too abstract an issue and advocates are too idiosyncratic to be pigeonholed. This is either a strength or weakness of privacy advocacy, depending on your perspective.

Comparisons between the environmental movement and privacy advocacy are common throughout the book. While the comparisons are at times instructive, it is more often the case that the differences are as great as the similarities. One notable difference is the lack of membership support for privacy while environmental groups benefit greatly from having members and individual contributors. Why? Bennett observes that membership organizations grow through use of mailing lists, an activity anathema to privacy advocates. But privacy groups

haven't prospered financially on the Internet either, a space where most feel at home. Fund raising on the Net seems largely unexplored.

Bennett's conclusions and advice for the future are reasonable, but they may not help anyone in the privacy community. As he notes, there is no worldwide privacy movement with the scale, resources, or recognition of the environmental, feminist, consumer protection or human rights fields. Privacy advocates themselves have different backgrounds, training, world views, politics, approaches, and values. They work together fitfully. His study makes it clear that there is no central focus for his advice, no clear path to the future, no evidence of overall organization, no continuing coordination among advocates. Bennett avoids use of the *herding cats* analogy, but it might have been appropriate.

In the end, Bennett says that he has "held a mirror up to the individuals and groups, who in the face of enormous social and technological pressures, have tried to advance a complex argument about the erosion of a fundamental human right" with few resources. This he has done, and he has done it well. What you see depends a lot on where you stand when you look into that mirror.

#####

A Brief History of a Privacy Incident

Robert Gellman
November 4, 2008
Version 1.0

A 1998 federal advisory committee hearing on a health privacy issue had a dramatic and long-lasting effect. While the hearing was not an event organized by or for the privacy community, the event offers a privacy case study worth retelling here, especially because it occurred in "pre-history" (mostly not available via the Internet).

In 1998, I served as a member of the National Committee on Vital and Health Statistics, an advisory committee of the U.S. Department of Health and Human Services. http://www.ncvhs.hhs.gov. The Department asked the committee to begin examining the requirement of the 1996 Health Insurance Portability and Accountability Act (a law better known for the health privacy regulation that it also mandated) for a health identifier for individuals. It was my perception at the time that the Department was so scared about patient identifiers that it tasked an obscure advisory committee to begin consideration of the issue in Chicago rather than in Washington where it might receive more attention. I was the "privacy" person on the Committee, but I didn't consider myself (then or now) to be a privacy advocate. Several other Committee members were also concerned about privacy, but most members came from the health data establishment.

On July 20, 1998, the first day of a two-day hearing, the New York Times ran a story by Sheryl Gay Stolberg titled: *Health Identifier For All Americans Runs Into Hurdles*. The story was a preview of the issue and the hearing. I do not know where the story came from. I did nothing to plant the story and was not interviewed by the reporter. The story was the key to later events.

Because of the story, several reporters and television producers came to the hearing. It is unlikely that press (other than trade press) would have attended the hearing but for the NYT story, especially television.

I came to the meeting prepared. Members of the committee rarely, if ever, offered opening statements other than a few words of welcome from the chairman. Because I was used to the hearing process from having worked as a Capitol Hill staffer for many years, I realized that an opening statement was essential. I read a 1000 word statement with the intention of laying down a marker for later committee work. I did not anticipate my statement would have any particular effect on the hearing or otherwise, but I wanted to wave the privacy flag.

My statement made two points. First, the stakes were far broader than just a patient identifier. I asserted that any identifier issued for use in health care would become a single national identifier just as the Social Security Number had become one. Second, the Committee, already on record favoring a patient identifier, was both biased and not representative of all stakeholders. No one ever cared about the second point.

I read my statement, and the hearing began. After an hour or so, there was a break. I was approached by a producer for a television station who said that the hearing was "boring except for you." He asked me to do an interview. Later that morning, a story (and perhaps part of the interview) ran, if memory serves, on CNN. That report brought many more reporters to the hearing. There were so many that when I returned from lunch, I held an impromptu press conference with many TV, radio, and print reporters. In the next day and a half, I gave numerous interviews to reporters. Other committee members did the same. Some members appeared the next morning (July 21) on Good Morning America. The Chicago Sun-Times ran a front-page story that same morning, with the headline filling the front page ("Medical ID Plan Spurs Privacy Fear"). There was much press coverage across the country. It seemed clear that the public did not welcome the prospect of a new health identifier and that the press saw the issue as a major one.

I do not recall what role privacy groups played in the aftermath of the hearing. The issue took off, broadened, and received high-level political attention. On July 31, 1998, Vice President Al Gore proposed an Electronic Bill of Rights that included a commitment not to implement a patient identifier until strong privacy protections were in place. He also announced that the Office of Management and Budget would be given responsibility for coordination of privacy issues. http://www.peterswire.net/privarchives/Gore%20on%20Admin.%20new%20privacy%20initiative.html. This eventually resulted in the March 1999 creation of a Privacy Counselor at OMB, a position held by Peter Swire until the end of the Clinton Administration.

With support from OMB, Congress passed an appropriations rider that limited the expenditure of funds for a patient identifier in the absence of specific legislative authority. It has remained in the law ever since. The current version found in Section 511 of Public Law 110-161 reads:

> None of the funds made available in this Act may be used to promulgate or adopt any final standard under section 1173(b) of the Social Security Act (42 U.S.C.

> 1320d-2(b)) providing for, or providing for the assignment of, a unique health identifier for an individual (except in an individual's capacity as an employer or a health care provider), until legislation is enacted specifically approving the standard.

The Department of Health and Human Services has scarcely taken a step in the direction of a patient identifier in the ten years. The legislative restriction has put a significant crimp in plans for a national health information network, a network being planned largely in secret with rhetorical respect for privacy but without any real attention to privacy and without active participation from the privacy community.

There may be a privacy lesson somewhere here, although the importance of coincidence and dumb luck should be part of that lesson. The New York Times story created an unexpected opportunity, my opening statement served as a spark, and the reporters present added gasoline. The accidental mixture had major consequences, but whether the conditions could ever be repeated with the same results is far from clear.