Technology and Privacy

Old Problems and New Challenges

By Marc Rotenberg

When the Section of Individual Rights and Responsibilities (IRR) was founded in the 1960s, the Congress was just beginning to explore an issue that would shape civil liberties debates for decades to follow. The original hearings on computer databanks and privacy were sparked by public concern about a proposal to establish a National Data Center that would contain detailed profiles on American citizens. Congress looked closely at how best to safeguard the fundamental right of privacy in a world increasingly transformed by new technology. The American Bar Association (ABA), working with technology experts and legal scholars, helped build the record and provide the insight that led to passage of the Privacy Act in 1974, perhaps our most important privacy law.

Still, it was clear that the challenges to privacy were not limited to the automation of personal information. Following the Supreme Court's opinions in *Katz v. United States,* 389 U.S. 347 (1967), and *Berger v. New York,* 388 U.S. 41 (1967), Congress also considered the need to establish comprehensive privacy protection for telephone communications. In describing electronic surveillance as "an investigative method of last resort," Congress created in Title III of the Omnibus Crime Control and Safe Streets Act of 1968 a comprehensive framework that established clear predicates for wire surveillance, limits on both the scope and duration of surveillance, judicial oversight, and meaningful public reporting requirements.

The ABA and IRR have an important responsibility to safeguard these key statutes in the face of new challenges. For example, following the September 11 attacks, President Ronald Reagan's former National Security Advisor, John Poindexter, recommended establishing a Total Information Awareness Program that would seek to combine all information on persons held throughout the federal government with that held in the private sector. He also proposed developing technology to link persons' e-mails to their DNA and to capture and analyze faces in public spaces. The effect of such a program would have been to eviscerate the Privacy Act. Although the program met with fierce opposition and Congress eventually suspended its funding, related initiatives have gone forward. The ABA and the Section should be contributors to the debate as Congress once again considers how best to safeguard privacy in an age of new technologies to profile and analyze Americans' private lives.

Similarly, the administration's assertion of the authority to conduct domestic wire surveillance without statutory authority or judicial oversight recalls the earlier congressional efforts to ensure that the government undertakes electronic surveillance within a legal framework that limits misuse and ensures public accountability. Many commentators have focused on the constitutional questions raised by the administration's position. But it is also important to consider the sweeping impact of that position on the statutory regime that Congress established and has updated periodically to safeguard communications privacy.

IRR has a particular interest in the current and future use of the Foreign Intelligence Surveillance Act (FISA), enacted in 1978 to address the narrow problem of Soviet spies operating within the United States. While recognizing that surveillance conducted for the purpose of gathering intelligence may be conducted under a regime different from the one established for criminal investigation, the Section successfully proposed and passed at the Midyear Meeting in 2003 an ABA policy urging the enactment of legislation for improved public reporting of governmental activity under FISA. The need is clear. The latest annual wiretaps report issued by the Administrative Office of the U.S. Courts contains more than one hundred pages on traditional wiretaps and provides detailed information about the cost, outcome, and impact of court-ordered wiretaps. But the report on FISA activity is little more than a page and simply states the number of FISA orders approved.

Looking ahead, the Section and the ABA will face many new technology-triggered challenges to privacy protection. For example, the Real ID Act, which would transform a state driver's license into a national identity card, already has drawn fierce opposition from civil rights organizations and immigration groups. Many suspect that the impact of such an identity system would fall disproportionately on minority populations and lead to expanded interrogation and detention of persons who would not be subject to traditional arrests. New systems of public surveillance, such as the camera systems that are found in many cities, soon could be linked to sophisticated databanks that match faces of residents, tourists, and political protesters in public places.

In *NAACP v. Alabama,* 357 U.S. 449 (1958), the Supreme Court struck down a state law that compelled the production of civil rights organizations' membership lists. It was a remarkable opinion that recognized the close ties between the right of privacy, political association, and social change. Safeguarding privacy in the years ahead will be no less critical than it was in the Section's early days.

Marc Rotenberg teaches privacy law at Georgetown University Law Center and chairs the IRR Committee on Privacy and Information Protection. After graduating from law school, he served as counsel to Senator Patrick J. Leahy (D-VT) on the Senate Judiciary Committee.