NATHAN BROOKS

Information Privacy

IT HAS BEEN well over 100 years since Samuel Warren and Louis Brandeis drew the outlines of privacy law for the century that followed. What they termed "the right to be let alone" (borrowed from a 19th-century torts treatise) became the guidepost for the evolution of the field over the next century. Whether discussing illegal searches or penumbras of privacy, judges always seemed to focus their analyses (whether they admitted it or not) on the simple but powerful idea that all of us exercise a certain sovereignty over our persons—an "inviolate personality"—that must be respected.

Since the years following World War II, however, a powerful undercurrent of thought has evolved with respect to privacy focused on personal information. The second half of the 20th century saw technological advances that made it increasingly possible to monitor and track persons as a result of the amazing amounts of personal identifying data that could be stored in ever more efficient ways. Governments that had always wanted to keep tabs on their citizens now had the means to do so and, with the paranoia that attended the Cold War, had a harrowing sense of urgency.

As innovations in computer technology continued at an incredible pace, authors and commentators began to warn of a future in which governments could use personal data to track and control the masses. To many, the right to be let alone was taking on a meaning different from the one that Warren and Brandeis had in mind. The new understanding of "information privacy" held that information is power, and the increasing availability of personal data created a real danger that this power would be abused.

The Orwellian vision of the omnipresent government eye never materialized, but the debate over information privacy did not die. Of course, personal information has real business value, and in place of the over-the-top warnings that "Big Brother" would use our personal information to exert control came the more realistic call for regulation of the business of personal information.

The rise of commerce over the Internet has exponentially increased the value of personal information. The business owner or banker identifies the customer not by his or her face but rather by the person's Social Security number or credit card number. Such information is often easy to steal and even easier to use. But personal data do not simply facilitate commerce; they also include information about criminal backgrounds and credit histories that employers, lenders, and others use in assessing the risks associated with their business decisions. Thus, in many instances, the person who complains that the availability of personal data leads to identity theft is the same person who requests a background check on the babysitter to ensure the safety of his or her children. The central question, then, is not how to prevent the collection and use of personal data completely, but rather how to make sure this information is used and secured properly.

The law has been slow to catch up with these concerns, and in this issue we not only examine some of the methods available for addressing these concerns but also identify a few of the difficulties that are lurking around the corner. Internet Protocol Version 6, for example, is set to greatly expand the amount of information the Internet can support, and yet relatively few people have even heard of the protocol, much less understand its importance.

The current legal framework in America is a patchwork solution at best, barely (if at all) able to curtail the rise of identity theft. Congress has been unable to pass comprehensive legislation designed to protect data, and the somewhat outdated Fair Credit Reporting Act remains one of the major federal laws related to information privacy. The U.S. Supreme Court recently had a chance to interpret this statute and, as discussed in this issue, the justices offered a revealing glimpse into their collective perspective of the act.

Advocates of legislation safeguarding the privacy of personal information can also look to the Gramm-Leach-Bliley Act, also imperfect, which can be enforced through private litigation or, somewhat controversially, enforced by the Federal Trade Commission. In this issue, two attorneys on the front lines of the battle over this act provide analyses of these separate enforcement mechanisms.

It seems clear that the federal government should enact comprehensive legislation designed to protect personal data, because in the absence of such a regime the states have enacted their own very different statutes. In searching for answers as to what a

federal program might look like, some commentators turn to Europe, where the horrors of the calculated mass murder that was the Holocaust loom large in the public consciousness, and information privacy is seen as a fundamental human right. An article in this issue examines the data protection regime implemented by the European Union to see if the European experiment offers lessons for the United States.

Many questions raised in this issue are familiar to readers of this journal, for example—

- How do we balance business needs with concerns over consumer protection concerns?
- In what persons or agencies should enforcement authority reside?

In reality, even though these questions may seem familiar, within the context of information privacy, the answers should be anything but. Information technology is already moving much faster than our legislators and regulators can respond to the advances, and those on the horizon threaten to put us even further behind.

In distinguishing information privacy from the original concept of the right to be let alone, Julie Cohen, author and Georgetown Law School professor of information privacy law, offered the following valuable advice: "The universe of all information about all record-generating behaviors generates a 'picture' that, in some respects, is more detailed and intimate than that produced by visual observation, and that picture is accessible, in theory and often in reality, to just about anyone who wants to see it. In such a world, we should all be cautious." **TFL**

Nathan Brooks serves as general counsel at U.S. ISS Agency, a security consulting firm in Charlotte, N.C., and is a member of the FBA Editorial Board.

Editorial Policy

The Federal Lawyer is the magazine of the Federal Bar Association. It serves the needs of the association and its members, as well as those of the legal profession as a whole and the public.

The Federal Lawyer is edited by members of its editorial board, who are all members of the Federal Bar Association. Editorial and publication decisions are based on the board's judgment.

The views expressed in *The Federal Lawyer* are those of the authors and do not necessarily reflect the views of the association or of the editorial board. Articles and letters to the editor in response are welcome.