Global Business & Development Law Journal

Volume 14 | Issue 2 Article 4

1-1-2001

Book Review Data Privacy in the Information Age

Jed Scully
University of the Pacific, McGeorge School of Law

Data Privacy in the Information Age†

*Reviewed by Jed Scully**

The reduction of all data to binary code, the subsequent capability of speed of light transmission, and the manipulation and reformulation of personal data leads one to seriously question the parameters of Samuel D. Warren and Louis D. Brandeis' definition of privacy as the "right to be left alone."[1] One hundred and eleven years ago, when this "right" to aloneness was formulated, a wave of electronic assaults on privacy had already begun. The development of telegraphy and telephony was in its infancy. Flash bulbs, high speed presses, movies and recording devices were making possible intrusions on one's aloneness at the will of the intruder. Although an American citizen's *expectation* of privacy in 2001 may be fairly close to the standard of one hundred years ago, the reality behind that expectation has been sharply reduced with the advent of the internet and digital marketing.

Simply put, there should be no realistic privacy expectation in a digital environment for any citizen's personal data. That is the clear conclusion that a reader will draw after reading Jacqueline Klosek's *Data Privacy in the Information Age.*

The neutrality of the book's title might lull one into a belief that personal information is confidential unless one voluntarily discloses private data. And yet, data and privacy, where consumers are concerned, are antagonistic concepts. Most consumers understand that information furnished "online," such as credit card data and personal identification numbers, will be used for the purposes of the particular transaction for which the information is furnished. Consumers are also aware that information for a particular Internet transaction may also be used for "marketing" purposes. A consumer may be less aware that personal information exchanged in face to face commercial or governmental transactions also are, as a matter of routine, uploaded to digital databases. Nearly every ATM withdrawal, credit card purchase, driver's license application, loan application, medical appointment, insurance data, property tax transaction, grocery purchase, and even cash transaction, whether conducted in person, online, or by mail is uploaded to electronic databanks.

Consumer reluctance to purchase goods and services online, because of anxiety about the misuse of personal data—such as social security account numbers, driver's

---

† By JACQUELINE KLOSEK, Quorum Books, 2000.

* Professor of Law and Director, Intellectual Property Concentration, University of the Pacific, McGeorge School of Law. J.D., B.A., University of California, Los Angeles.

1. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 213 (1890).

license numbers and other identifiers– has caused slower growth for online sales than would be expected, especially given the obvious advantages and convenience over face to face transactions. This reluctance would spread if consumers fully appreciated the extent to which personal data is gathered, sliced, diced, traded, sold, rented, mined, archived, and transmitted to agencies and individuals unconnected to the particular transaction. Consumers would be truly amazed if they understood the scope of commercial traffic in their personal data. If they would like to confirm their suspicions, they should definitely review Klosek's book.

At the outset, Klosek emphasizes the fact that the internet is responsible for the great increase in concerns about privacy and data protection. Personal information has always been collected from consumers, but the development of the internet has provided a very efficient, effective, and anonymous method for collecting personal data with significant commercial value. The author points out that most of this activity is unknown to the person inadvertently providing the data.

Next, Klosek relates two general governmental approaches to privacy concerns about the proliferation of personal data on the internet. These two approaches are exemplified by the European Union (EU) and the United States (U.S.).

The first level of legislative response is that of the European Union and various associated states which resulted in the EU Data Protection Directive.[2] Beginning in 1968, some two decades before the widespread use of the Internet, there were a series of European conventions, agreements, and treaties providing for enforceable international protection for individual privacy rights in personal data.[3] Twenty-four European nations ratified the convention on privacy protection between 1981 and 1997.[4]

The convention provides that an individual has a right to know about personal data which is collected and the right to correct erroneous data. In addition, the convention authorizes monetary compensation for the collection and dissemination of inaccurate data. Most significantly, there are provisions restricting the dissemination of data to other countries which do not offer equivalent levels of protection. A number of amendments expanding and refining these basic protections have been enacted. The European Union adopted this Convention as the Data Protection Directive in 1998, thereby greatly expanding the scope and enforceability of the Convention.[5]

On the other hand, the United States does not have comprehensive national legislation regarding the privacy protection of personal data. Klosek uses the United States to illustrate a second government approach to privacy. Where privacy

---

2. The European Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data. Directive 95/46 EC of the European Parliament and of the Council of 24 October 1995. The Data Protection Directive came into force in the European Union on October 24, 1998.

3. KLOSEK at 13. *See generally* Council of Europe's Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, 1981.

4. *Id.*

5. *See supra* note 2.

protection is found in the United States, it is normally found in state rather than federal law. By comparison to the EU, American culture is considerably more tolerant concerning the harvesting of personal information for commercial purposes. Perhaps this is because commercial interests, including the banking, finance, health care, insurance and marketing industries strongly resist legislative initiatives which seek to impede the collection and dissemination of personal data, either internally within a company, or its sale and dissemination to others.[6]

At this point, Klosek asserts that the diversity of perspectives about personal data collection between the European Union and the United States has become increasingly problematic with the growth of the Internet. In order to provide transborder transmission of data, the United States has negotiated "safe harbor" exemptions for data flow between the United States and the European Union in order to satisfy minimum EU privacy protection standards.[7] Ironically, these safe harbor provisions offer greater protection than is common within the United States.

In time, the author turns her attention to the U.S. data collection privacy standards which emphasize self-regulation by the affected industries and companies. The U.S. governmental position is that self regulation—with oversight from the Federal Trade Commission—is sufficient, and that providing individuals with unrestricted data to their own personal data is too burdensome for commercial interests.

Nevertheless, Klosek concludes that there is significant incentive to American-based commerce to avoid misuse, or even the *perceived* misuse of private data, in order to bypass governmental intervention and oversight. Most importantly, companies should perpetuate greater privacy protections so as to eliminate consumer avoidance of online transactions if consumers feel that the privacy of their personal data will be shared beyond the entity with which they are dealing. Wal-Mart recently announced that it would no longer traffic externally in customer data collected at points of sale.[8] Inasmuch as WalMart is the largest volume retailer in the United States, this signals a significant trend.

Scott McNealy, chairman and CEO of Sun Microsystems, commented that on the Internet, "You have zero privacy–get over it!"[9] That is an exhortation which

---

6. In addition to issues of an individual consumer's rights to privacy and the attendant right of publicity, there could be an argument that consumers have a protectible interest in their personality rights against commercial appropriation by another. This right might also be expressed as a moral right of integrity and attribution. *See, e.g.*, Article 6bis, Berne Convention for the Protection of Literary and Artistic Works (Paris Act, 24 July 1971) and the Berne Convention Implementation Act of 1988 (Pub. L. 100-568, 102 Stat. 2853).

7. In March 2000, the United States and the European Union announced provisional agreement on the Safe Harbors program providing greater legal certainty for transatlantic data transfers. *See* KLOSEK, at 178-82.

8. *See* Dana Blankenhorn, *100 Trillion Bytes of Customer Data: How Marketers' Database Muscle is Growing, at* wysiwyg://73/http://adagespecials.com/data1.shtml (last visited Oct. 30, 2001) (on file with *The Transnational Lawyer*).

9. John Markoff, *Growing Compatibility Issue: Computers and User Privacy*, N.Y. TIMES, Mar. 3, 1999, at A5. *See* Polly Sprenger, *Sun on Privacy: 'Get Over It', at* http://www.wired.com/news/politics/0,1283,17538,00.html (last visited Oct. 30, 2001) (on file with *The Transnational Lawyer*).

American consumers are increasingly less likely to accept. Moreover, the reluctance of U.S. governmental entities to "fix" privacy with legislation may also be a recognition of the limits of geographical statutes to deal with transnational cyberspace. But commercial interests, operating in a global environment, are beginning to appreciate the need to balance the demand for market data with consumers' resistance in providing personal information without their advance approval.

All in all, Jacqueline Klosek merely lays out the facts. Policy makers and ordinary consumers should not allow historical attitudes and fantasies about personal privacy affect the current reality of twenty-first century data collection. In the short run, the national trauma of September 11, 2001 will undoubtedly result in statutory and regulatory changes which will increase direct governmental interest and activity in data collection and impose limitations on the uses of personal data by private and commercial interests.[10] Even with those contemporary personal, public, and governmental changes in attitude about data privacy, Klosek's book remains a useful reference work in tracking the policy and politics of personal data collection and dissemination.

10. On October 25, 2001, President Bush signed Anti-Terrorism legislation allowing roving wiretaps on persons suspected of terrorism, monitoring of e-mail messages and traffic by terrorism suspects, the monitoring of digital traffic by financial institutions to detect money laundering, and other provisions. *A Nation Challenged,* N.Y. TIMES, Oct. 26, 2001, at B1-B3.