The Legal Report

By Richard L. Field, Esq.
Email: field@pipeline.com

Mr. Field is a U.S. attorney specializing in payment systems and electronic commerce. He chairs the Electronic Commerce Payment Committee of the American Bar Association, Section of Science and Technology, and sits on its Section Council. He is an Affiliated Research Fellow of the Institute for Tele-Information at Columbia Business School. Mr. Field has served as a U.S. delegate-adviser to the United Nations Commission on International Trade Law, Working Group on Electronic Commerce.

My report this month focuses on personal privacy, perhaps the most volcanic social issue in electronic commerce. It surveys the U.S.'s historical approach towards privacy protection.
President Clinton has recently advocated, for the U.S. and the rest of the world, a government "hands-off" policy towards privacy protection, as well as most other on-line regulation. Such a policy rewards the business community, a significant engine for national ecommerce growth, while also reflecting the practical difficulties of drafting laws at this stage.

In the article I have reprinted, I take the position that this "hands-off" gift is a two-edged sword. The vacuum created by a government's failure to protect consumers will certainly be filled, most likely by distrustful consumers who now have the means to make themselves heard. The business community may yet find that it prefers the certainty of regulation to ambush over the net.

The Great Mining Disaster of '99

First published in the Electronic Banking Law and Commerce Report, November/December 1997

Great fortunes were built in the nineteenth century by those who knew how to possess and mold the riches of the earth. Gold, silver, coal, timber and oil fueled the Industrial Revolution, and provided its raw materials and funding. One downside: the earth can be unpredictable and ruthless, swallowing players and innocents alike.

Nothing's changed. Our roads are now paved with information, not cobblestones from the receding cliffs on the Hudson. What is receding these days is a vision—or an illusion—of a world safe for privacy, selective anonymity, and the inalienable right to be left alone. Wherever the truth may lie, it is clear that privacy concerns, coupled with the ability to broadly discuss and widely disseminate them, continue to awaken the consciousness and stir the aggressive tendencies of an uneasy populace.

The U.S. public is famous for its historical ambivalence towards personal privacy. As a result, we have no comprehensive statute or directive to ensure privacy rights, but rather a loosely woven set of rules and socially accepted practices. Though it may be an overgeneralization to say our European neighbors trust governments but not corporations with their personal lives while our loyalties are reversed, to some degree this pattern is reflected in each of our laws.
The Privacy Act of 1974 (5 USC 552a), for example, broadly protects personal information in Government data

banks. It embodies principles of fair information practices first set forth in Computers and the Rights of Citizens, a report published in 1973 by the former U.S. Department of Health, Education, and Welfare. These principles include:

1. There must be no secret personal data record-keeping system.
2. There must be a way for individuals to discover what personal information is recorded and how it is used.
3. There must be a way for individuals to prevent information about themselves, obtained for one purpose, from being used or made available for other purposes without their consent.
4. There must be a way for individuals to correct or amend a record of information about themselves.
5. An organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for its intended use and must take reasonable precautions to prevent misuses of the data.

The former Office of Technology Assessment noted in 1994 that the increased computerization and linkage of information maintained by the Federal government may not be addressed by the Privacy Act. [U.S. Congress, Office of Technology Assessment, Information Security and Privacy in Network Environments, OTA-TCT-606 (Washington, DC: U.S. Government Printing Office, September 1994)].

Although it is addressed mainly in the context of specific industries or activities, if at all, the idea of a right to privacy against private sector intrusions has been kicking around the academic world for some time. Warren and Brandeis discussed the right to be 'let alone" back in 1891 [Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193 (1891)]. Prosser concluded that no right to privacy existed under U.S. constitutional law, but identified various tortious invasions of privacy [William Prosser, Privacy, 48 Calif. L. Rev. 383 (1960)]. Starting in 1965, the U.S. Supreme Court recognized a limited Constitutional right to privacy [Griswold v. Connecticut, 381 U.S. 479 (1965)], notably in the bedroom. Based on the Fourth Amendment's prohibition against unreasonable searches and seizures and depending on work environment, employees may also have a reasonable expectation of privacy in the contents of their desks [O'Connor v. Ortega, 480 U.S. 709]. The Fourth Amendment's reasonable expectation of privacy has been held inapplicable, however, to bank records [United States v. Miller, 425 U.S. 435 (1976)].

The U.S. financial sector retains an enviable degree of public trust, due in no small part to its traditional sensitivity towards issues of privacy. This sensitivity is encouraged through federal and state privacy statutes that have developed over the past thirty years, such as the Right to Financial Privacy Act of 1978 (12 USC 3401 et seq.) and similar provisions in the tax law (26 USC 7609-7610), which govern access to financial industry information by federal government agencies and the IRS; the Fair Credit Reporting Act of 1970 (15 USC 1681 et seq.), which governs the information practices of the credit bureaus and other consumer reporting agencies, as well as the sharing of affiliate information by financial institutions and the use of consumer reports; and the Electronic Fund Transfer Act of 1978 (15 USC 1693 et seq.), which requires a general disclosure of the circumstances under which a financial institution may disclose information to third parties concerning a consumer's bank account.

The states protect personal privacy in various ways, also to a limited degree. Some state constitutions contain express privacy protections. Others protect privacy where a reasonable expectation is deemed to exist, at times going further than the Federal standard. State common law has evolved to protect some disclosure of financial information, and a few states (including Massachusetts and Wisconsin) have adopted general privacy statutes, while others (including New Jersey, California and Maine) have rules targeted to credit reporting, electronic fund transfers, or other financial industry practices.

Naturally, the electronic information world is the focus on much of the more recent privacy legislation. The Computer Security Act of 1987 established a Computer System Security and Privacy Advisory Board within the Department of Commerce, to identify safeguard issues and to advise on security and privacy issues pertaining to Federal computer systems (see 15 USC 278g-4), and required each Federal agency to identify its computer systems containing sensitive information (see 40 USC 759 note). The Electronic Communication Privacy Act (18 USC 2510) prohibits certain third party interceptions of communications, access to stored communications, and disclosures of communications, without the consent of at least one party to the communication, or unless there is a valid business use. Some states have modeled their own wiretapping statutes after this act, sometimes eliminating the business use exception or requiring the consent of both parties.
The Privacy Working Group of the NII Task Force's Information Policy Committee issued a 1995 report, "Privacy

and the Information Infrastructure: Principles for Providing and Using Personal Information" (available at <http://www.iitf.nist.gov/ipc/ipc/ipc-pubs/niiprivprin_final.html>). The report identifies a number of general principles, including:

I. General principles for all NII participants:

1. Information Privacy Principle: Personal information should be acquired, disclosed, and used only in ways that respect an individual's privacy.
2. Information Integrity Principle: Personal information should not be improperly altered or destroyed.
3. Information Quality Principle: Personal information should be accurate, timely, complete, and relevant for the purpose for which it is provided and used.

II. Principles for Users of Personal Information:

1. Acquisition Principles: Information users should -- (i) assess the impact on privacy in deciding whether to acquire, disclose, or use personal information; and (ii) acquire and keep only information reasonably expected to support current or planned activities.
2. Notice Principle: Information users who collect personal information directly from the individual should provide adequate, relevant information about -- (i) why they are collecting the information; (ii) what the information is expected to be used for; (iii) what steps will be taken to protect the confidentiality, integrity, and quality; (iv) the consequences of providing or withholding information; and (v) any rights of redress.
3. Protection Principle: Information users should use appropriate technical and managerial controls to protect the confidentiality and integrity of personal information.
4. Fairness Principle: Information users should not use personal information in ways that are incompatible with the individual's understanding of how it will be used, unless there is a compelling public interest for such use.
5. Education Principle: Information users should educate themselves and the public about how information privacy can be maintained.

III. Principles for Individuals Who Provide Personal Information:

1. Awareness Principle: Individuals should obtain adequate, relevant information about -- (i) why the information is being collected; (ii) what the information is expected to be used for; (iii) what steps will be taken to protect its confidentiality, integrity, and quality; (iv) the consequences of providing or withholding information; and (v) any rights of redress.
2. Empowerment Principles: Individuals should be able to safeguard their own privacy by having -- (i) a means to obtain their personal information;
(ii) a means to correct their personal information that lacks sufficient quality to ensure fairness in its use; (iii) the opportunity to use appropriate technical controls, such as encryption, to protect the confidentiality and integrity of communications and transactions; and (iv) the opportunity to remain anonymous when appropriate.
3. Redress Principle: Individuals should, as appropriate, have a means of redress if harmed by an improper disclosure or use of personal information.

Based on these principles, the Committee prepared and issued for public comment an April 1997 paper, "Options for Promoting Privacy on the National Information Infrastructure", which explores the growing public concern about personal information privacy, comprehensively reviews information privacy laws and practices, and calls for a reexamination of the proper balance between the competing values of personal privacy and the free flow of information in a democratic society. It recognizes the reactive and patchwork nature of information privacy protection efforts in the U.S.

The Clinton administration has focused on these documents in its July 1, 1997 Framework for Global Electronic Commerce (available at <http://www.whitehouse.gov/WH/New/Commerce/read.html>). Recognizing the critical importance of data protection and privacy, it goes on to support private sector efforts now underway to implement meaningful, consumer-friendly, self-regulatory privacy regimes, while backing away from government protection of privacy. It warns, however, that if effective privacy protection cannot be provided through self-regulation, it will reevaluate this policy in the face of increasing pressure to play a more direct role in safeguarding consumer choice

regarding privacy online.

Where does this leave us? The administration's "hands off" position will be increasingly challenged by Congress, which tends to address consumer issues on a more human scale. Trade friction between the U.S. and the European Community can only escalate, as the U.S. comes to see the EC's Data Privacy Directive as a non-tariff barrier to trade, while the EC sees itself as holding the higher moral ground. Indeed, the increasingly tough U.S. position may readily become a rallying point around which the EC can organize its opposition to U.S. domination of the Internet.

Most ominously, we are starting to see more organization at the grassroots level, a sort of "privatization" of privacy and consumer protection. As Lexis-Nexis, the Social Security Administration, and the credit card organizations (to name a few recent examples) can attest, the power of a wrathful public venting its displeasure over the Internet can be unpredictable, immediate, and more challenging to corporate planning efforts than the regulatory process. Absent the paternal protection of government, and suspicious of the good faith of industry, the grassroots has shown that it can protect itself. Once uncorked, this genie will not easily be rebottled. Uncertain of what the public will stand for, corporate America is nevertheless irresistibly lured by the same technologies to collect and use information in creative ways. An almost certain recipe for an impending data mining disaster. Try not to be the one caught.