2001

Unnecessary Privacy

Carl Felsenfeld
Fordham University School of Law, cfelsenfeld@law.fordham.edu

Follow this and additional works at: http://ir.lawnet.fordham.edu/faculty_scholarship

Part of the Communications Law Commons

Recommended Citation
UNNECESSARY PRIVACY

Carl Felsenfeld*

An individual’s right to privacy in an electronic society has gained international attention as a booming new field. Its birth may roughly be marked to coincide with the birth of the Internet. The flow of information without limit or boundary has raised concerns with the consumer spokespeople in the Western World that personal information about them may flow as easily as general information about Machu Pichu, Keynesian economics, or Harvard College. The fear is that will cause individuals harm, ranging from personal embarrassment to a loss of civil liberties. Therefore, movements are developing to limit this flow of information. The direction that this movement should take is the subject of controversy. This article argues that our right to the privacy of electronic information is of no real consequence to us and has largely already been lost. Furthermore, most of the information about us should not be squeezed to the vest like a winning poker hand, but, rather, should be happily publicized. What had been thought of as dirty little secrets, should better be seen as fresh air.

I. The Problem

The United States and Europe view the treatment of personal electronic information differently. In the United States, studies of personal information and privacy are now commonplace. A White House Infrastructure Task Force formed in 1993 wrote one document of some significance, which was released over the signatures of President Clinton and Vice President Gore. Titled A Framework for Global Electronic Commerce,¹ the document is peculiarly unsatisfying. Prominent in it is the statement “Americans treasure privacy.” Yet, when specifics are called for to enjoy the treasure, the Framework presents as a “principle” the industry-pleasing:

[G]overnments should encourage industry self-regulation wherever appropriate and support the efforts of private sector organizations to

* Professor of Law, Fordham Law School.

develop mechanisms to facilitate the successful operation of the Internet. Even where collective agreements or standards are necessary, private entities should, where possible, take the lead in organizing them.2

There are many people, particularly those representing consumer interests and on federal and state legislatures, who believe that in areas like privacy protection, industry self-regulation is really no regulation at all. Sides have been drawn and there are those who are convinced that consumers will receive privacy protection only if there is law, including regulation, that prescribes levels of protection well beyond those that exist today. On the other side, there is a body of opinion that believes only the give and take of the free enterprise system can achieve the appropriate level of regulation. The consumer representatives tend to believe that self-regulation is no regulation at all, essentially allowing the foxes to rule the hen house.

In the United States, a disorganized scatter of laws and regulations governing and controlling consumer privacy exists.3 Some exist at the federal level,4 but many more at the state level. Among state laws are those that require consumer consent in advance before personal information about them may be transferred, while others provide much lighter levels of protection. Some states have no privacy laws at all. A pervasive layer of common law doctrine, however, exists according consumers rights as against institutions to which they give personal information. This doctrine is based upon such factors as actual or presumed agreements between consumer and institution, and reasonable consumer expectations deriving from the nature of their relationship with business institutions.

One of the major efforts to voice the need for heavier privacy regulation was the Federal Trade Commission's (F.T.C.) May 2000 report to Congress titled Privacy Online: Fair Information Practices in the Electronic Marketplace.5 The report was

---

2. Id.
the F.T.C.’s third on the subject and essentially consistent with an earlier 1998 report that was highly critical of industry practices concluding that the industry had “fallen far short of what is needed to protect consumers.” The 2000 report was based upon industry recognition of what the F.T.C. considered the four principles of adequate privacy protection: notice (to the consumer of industry privacy procedures), choice (of the consumer to the use of information about him), access (by the consumer to information retained about him), and security (maintained by industry in consumer information).

The report acknowledges that, because of the wide variety in the nature of industry practices and the difficulties of matching and tabulating responses, “[t]here are limits . . . to the value of this data.” Nevertheless, the F.T.C. concluded that “only a small percentage of sites are providing protection in core areas.” Among business representatives, the F.T.C. is usually considered to be slanted in favor of consumer interests. For example, the Democratic influence dominated the F.T.C. during its privacy releases. We are unaware of any change of heart on privacy matters the F.T.C. may have experienced in view of more recent political changes.

Not to be accused of a pro-consumer bias in financially-related matters is the American Bankers Association. Generally allied with the policies of the aforementioned Clinton/Gore framework, the American Bankers Association believes that the current structure of privacy protection laws now existing in the United States is essentially sufficient and that industry self-regulation should govern change, to the extent change is called for. In 1997, the American Bankers Association published a set of eight Privacy Principles for banks to follow to establish a satisfactory level of customer financial privacy. The guidelines are:

1. Recognition of a Customer’s Expectation of Privacy. This includes the possibility of explaining the principles of financial privacy to customers prior to a banking relationship.

2. Use, Collection and Retention of Customer Information Only if the Institution Believes the Customer Will Benefit.

6. PRIVACY ONLINE, supra note 5, at 11. One-fifth of the sites currently provide protection in core areas. Id.

7. Id. at 12.
Among potential benefits to consumers is the institutions' ability to offer consumers products, services, and other opportunities.

3. Maintenance of Adequate Information. Financial institutions should ensure that the consumer information they retain is accurate.

4. Limiting Employee Access to Information. Only those employees with a legitimate business reason to see consumer information should have access to it.


6. Restrictions on the Disclosure of Account Information. Consumer customer information should be disclosed to third parties only for certain prescribed purposes including: (1) when it is necessary to assist the customer in accomplishing his own transaction; (2) when the customer requests it; (3) when the law requires disclosure; or (4) when the customer has been informed.

7. Maintaining Customer Privacy in Business Relationships With Third Parties. Institutions should require the third parties legitimately receiving the customer information to maintain similar standards.

8. An Institution's Privacy Principles or Policies Will Be Made Known to the Customer.

The American Bankers Association followed its statement of Privacy Principles with a more broad-based consideration of the American privacy law. They issued their statement, titled Financial Privacy in America, in June 1998. The statement indicates that the U.S. banking industry is highly regulated, and that this regulation “[h]as been successful in providing adequate consumer privacy protection, while permitting the free flow of information that is vital to not only the financial services industry, but our economy as a whole.” The study goes on to emphasize that privacy regulation in the United States is not based upon a single source of law, but rather “[a]n extensive combination of overlapping federal and state laws governing personal privacy.”

8. See CARL FELSENFELD, INTERNATIONAL BANKING REGULATION VI-59 (Juris ed. 2000).


These enactments do not all centrally concern privacy. For example, the Federal Trade Commission Act establishes a major federal bureaucracy for the regulation of trade, both consumer and commercial and does little more than provide an area of jurisdiction for consumer privacy consideration. Its basic substantive direction is a command that the F.T.C. act to prevent "unfair" or "deceptive" practices in the marketplace. The American Bankers Association study, as an Appendix, also charts the state laws protecting privacy and notes enactments in four separate areas: right to financial privacy acts; laws prohibiting recording credit card numbers on checks; laws limiting use of confidential customer information in insurance sales; and laws limiting use of social security numbers.11

Interest in personal privacy has been increasing for some years. It has escalated since the widespread availability of credit cards and the transmission of card-related information over the Internet. The public joinder into card-related activity has essentially made real privacy unavailable, a fact that is only gradually


11. See American Bankers Association, Consumer Privacy: A Free Choice (Sept. 2001), at http://www.pacificresearch.org/. Another broad-based privacy study is titled Consumer Privacy: A Free Choice Approach released September 2001, by the Pacific Research Institute for Public Policy, a conservative think-tank. Id. It warns that much of the privacy legislation pending in Congress and the state legislatures will harm rather than help consumers. Id. The study cautions that new laws may lull consumers into feeling safe, but the only way to guarantee protection is to safeguard themselves. Id.
being recognized. Attention to privacy issues has escalated not only in the United States, but, perhaps to an even greater extent, in the European Community as well. In the United States, we tend to see fundamental civil liberties law as protecting us as individuals from governmental intrusion. For example, the First Amendment to the Constitution prohibits the federal government from interfering with the public's rights of free expression, religion, and assembly. Much of our reliance upon self-regulation in privacy protection, as contrasted with externally imposed law legislators and regulators design for our protection, undoubtedly derives from our fundamental suspicion of government and desire to be free of its controls.

In the European Community, public feelings about government are not quite the same. Government on the European continent is perceived more as the protector of individual needs, rather than an entity who interferes with those needs. Europe is more comfortable with a socialist approach where government protects an individual's liberties, basic needs such as food and shelter, and continuing rights to employment. Thus, it should come as no surprise that the European Union (EU) enacted a Union-wide Data Protection Directive (Directive) in 1995\(^1\) purporting to protect rights in privacy as against industry-created interference.

The Directive was stated to deal with two basic aspects of data employment: “[t]he processing of personal data and (on) the free movement of such data.” In Whereas clause number 3, the Directive asserted that “[p]ersonal data should be able to flow freely from one Member State to another, but also that the fundamental rights of individuals should be safeguarded.” That these two objectives should turn out to be inconsistent apparently presented no problem. The Directive heightened American interest in privacy law largely because a provision addressed information transfer from an EU state to a foreign state. Whereas clause number 57 reads in major part: “[t]he transfer of personal data to a third country which does not ensure an adequate level of protection must be prohibited.”

Aware of the close relationship of European and American financial affairs, the EU Parliament considered the protection American privacy law provided consumers and, while not specif-
ically asserting that American privacy laws were inadequate under the Directive’s standards, obviously did not consider “adequate” the overall structure of U.S. law. Consequently, subject to variations in U.S. law or some form of concordat between the EU and the United States, a risk existed that personal information acquired and stored in the EU could not be transferred to the United States. This could create major problems. A large international bank with customers in the EU and processing centers in the United States could not transmit information concerning those customers across the Atlantic. A credit reporting company could not report personal credit information gathered in Europe to the United States.

II. European Union Level of Protection

Basic to privacy protection in the EU, the Directive prescribes that personal data may not be processed without the express consent of the person involved. The Directive expressly provides, “[p]ersonal data may be processed only if (a) the data subject has unambiguously given his consent.” This has become known as the “opt-in” standard with the ability to collect personal data subject to the will of the individual involved. When law in the United States exists and, in general, a financial institution has undertaken to grant rights of privacy to its customers, an opposite standard, generally called “opt-out,” is in favor. Under the “opt-out” approach, an individual has the right to demand that the collection and/or the commercial use of personal information about him be stopped or curtailed.

The Gramm-Leach-Bliley Act of 1999, whose major contribution to American law was to liberalize the powers of bank

---


14. Council Directive 95/46/EC, supra note 12, art. 7. There are other bases for the collection of personal information such as where it is necessary to perform a contract to which the subject is a party, or where it is required to perform a legal obligation. Id. Member States of the EU may also establish additional categories for their own purposes. Id. These other provisions do not affect our argument.

15. Dep’t of Transportation and Related Agencies Appropriations Act, § 350, 106 Pub. L. No. 69, 113 Stat. 686 (1999). An exception to the prevailing approach is a federal law requiring states, as a condition to receiving federal highway funds, to require “opt-in” consent from individuals before information about them in motor vehicle records may be used commercially. Id.

holding companies, has certain provisions relating to consumer privacy. These are of the “opt-out” variety. The Act provides in pertinent part:

A financial institution may not disclose nonpublic personal information to a nonaffiliated third party unless . . .
(B) the customer is given the opportunity, before the time that such information is initially disclosed, to direct that such information not be disclosed to such third party; and
(C) the customer is given an explanation of how the consumer can exercise that nondisclosure option.17

These requirements are embodied in regulations issued by the appropriate regulators: for banks, principally the Federal Reserve Board, the Comptroller of the Currency, and the Federal Deposit Insurance Corporation; for institutions that are not banks, principally the F.T.C.18 Notices were distributed to institution customers before July 1, 2001, the date prescribed by Gramm-Leach-Bliley.19

The U.S. position on privacy is thus the scattering of laws and regulations described in the American Bankers Association paper20 and the Gramm-Leach-Bliley “opt-out” notices. It has been generally assumed that these laws and regulations will not provide the level of adequate protection to consumer information that the Directive requires. Such action that has been taken in Europe and the United States since the Directive has been based upon that assumption.

A surprising absence of interference by European authorities with information flowing from the EU to the United States has occurred. An early example was action in 1997 by the German Deputy Commissioner of Data Protection preventing Citicorp (now Citigroup), the New York bank holding company, from moving information from Germany to the United States. This actually was before the Directive’s effective date, but imposed under prior German law containing a similar principle.21

An agreement entered into by Citicorp specifying a satisfactory

17. Id. at § 502.
20. See generally Consumer Bankers Association, supra note 9.
level of protection provided to the information received related to this problem. The concept of individual agreements according EU interests an acceptable level of privacy protection has been discussed from time to time over the years, but has not achieved any general level of acceptance.

The difference between the level of privacy protection required in Europe and that granted in the United States cannot be overstated. For one thing, there is an EU-wide document, the Directive, prescribing in general terms the appropriate level of protection, including the "opt-in" standard. The Directive requires that the Member States "determine more precisely the conditions under which the processing of personal data is lawful."22 Nevertheless, the basic standards are the same across the EU. In the United States, much of the applicable law is established at the state level and, consequently, different depending upon the state affected. The federal law that does exist addresses particular problems and not privacy itself.

American state law is free of the "opt-in" standard. The concept has received some attention in California where, as of this writing, September 2001, an "opt-in" bill passed the Assembly Appropriations Committee.23 American bankers are opposed to an "opt-in" standard of data protection. One objection is based upon the monumental record keeping and derivative expense that would be required if every customer were requested to give separate consent.

Amusing to an American lawyer, the Directive's "opt-in" standard appears not to be observed. Privacy expert Fred H. Cate of the University of Indiana Law School writes:

First, while it is true that European nations are required under the European Union data protection directive, which took effect in 1998, to condition the collection, use, or transfer of personal information on explicit consent, there is little evidence that any have, in fact, done so. European data protection officials have repeatedly pointed out the impossibility of doing so. Instead, Europe has used a concept of "implied explicit consent"—if individuals are told of the intended data collection or use and do not object, then surely, European data protection officials argue, they must have opted-in.24

Professor Cate’s information is consistent with a 1999 article by Professor Amitai Etzioni of George Washington University that provides:25 “[i]t seems that this EU directive is one of those laws that is enacted to keep one group - privacy advocates and their followers - happy and, as a rule, is not enforced so that commerce and life can continue.” This casual disregard of law is difficult for an American law professor to accept, although other sources mentioned in the articles of both Professor Cates and Etzioni (and subsequent telephone conversations between the author and both of them) support the conclusion. Based upon these insights, however, it is not unreasonable to conclude that the same legal requirement can be accepted with ease in the EU and represent a destructive bureaucratic force in the United States.

A comparative study of the EU and the United States in this regard is necessary. A strong feeling exists that something is missing from the reports cited above and more is to be learned before conclusions can be reached. Is it a different feeling about law on the two sides of the Atlantic, or is it ignorance in the United States of what is occurring in the EU? Perhaps, as another possibility, the EU reaction can be ascribed to the particular relationship of EU banks and their customers. It has even been suggested that EU banks may prefer not to get their customers’ consent to the economic use of otherwise private information so that they are not encouraged to give or sell the information to other institutions, banks or otherwise. In that manner, the EU banks will be more likely to retain their existing customer relationships and be relieved of the need to compete with those who are less informed.

Relationships between the EU and the United States are remarkably unstrained in view of the Directive’s requirements and the apparent shortfall in American law. The United States has not seen any organized restriction upon the transfer of EU personal information across the Atlantic, despite what appears to be the opportunity to impose restraints. This result is highly reminiscent of the situation that exists in the banking field under the EU Second Banking Directive,26 which provides that a foreign bank may not branch into the EU unless EU banks may

branch into the foreign country. The United States, however, has significant restraints upon entry by foreign banks, particularly at the state level. Robert L. Clarke, a prior Comptroller of the Currency, stated in a report to Congress:

The more significant disparities between U.S. treatment of domestic and foreign banks occur at the state rather than the federal level. Several states - Florida, New Jersey, and Virginia, for example - and the District of Columbia restrict entry by foreign bank holding companies. In other instances, regional banking compacts exclude participation by foreign banks.27

Based on various informal conversations with EU banking officials, they are well aware of the absence of reciprocity in the United States and their ability to exclude American banks from the EU. On the other hand, this is not their objective. They would much rather have a flourishing interchange of banks across the Atlantic. Thus, given the general policy of “national treatment” in the United States, the EU prefers to look at those state restrictions as relatively minor deviations that can be (at least for the time being) ignored. The same may apply to the Data Protection Directive and its requirement for adequate protection. It is more seemly that information travel between our two continents and that we deal with the problem to find resolutions short of blockade.

The most focused work undertaken in the United States to bridge the gap with the Directive has been the Department of Commerce’s Safe Harbor Principles (Principles).28 Released on July 24, 2000, the Principles, together with some relevant supporting materials including a presentation of how an organization’s commitment to them will be enforced in the United States, were forwarded by Commerce Department Office of International Trade Administration/Trade Development to the European Commission in Brussels with a request that the Commission determine the Principles’ adequacy under the Directive. The forwarding letter stated: “[o]ur expectation is that the European Commission will determine that this safe harbor framework provides adequate protection for the purposes of Article 25.1 of the Data Protective Directive and data transfers from the

27. Id. See also THE CONFERENCE OF STATE BANK SUPERVISORS, A PROFILE OF STATE CHARTERED BANKING, Part V (18th ed. 2000).
European Union would continue to organizations that participate in the safe harbor.”

The Principles’ underlying approach is to commit a domestic organization in the United States to honor them. The Principles would thereby achieve compliance with the Directive and the U.S. organization could receive personal information from the EU. Thus, the term “safe harbor.” Compliance with the Principles is entirely voluntary. Typically an organization will rely upon self-regulation to comply with the Principles. When an organization undertakes to rely upon the Principles and fails to do so, however, it may be subject to action under Section 5 of the Federal Trade Commission Act prohibiting unfair and deceptive acts.

Organizations wishing to take advantage of the Principles must commit adherence to seven separate principles summarized in the underlying document. It requires that they apply those principles to personal data acquired after they enter the safe harbor system. The specific principles and a few words about each follow:

1. Notice. An organization must inform individuals about the purposes for which it collects and uses information. It must inform about how to contact the organization with any inquiries or complaints and the types of third parties to which it discloses the information.

2. Choice. Individuals must have the right to “opt out” from use and third party disclosure of the individuals’ information. For sensitive information (i.e. personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or information specifying the individual’s sex life), the Principles deviate from their general “opt-out” position and require that the individual be given an explicit – “opt-in” - choice.

3. Onward Transfer. Organizations must ensure that third parties to whom it transfers personal information have relatively the same level of responsibility - that, for example, they subscribe to the Principles themselves or agree to do so - in essentially the same manner as the initial organization. If an organization conforms to this principle, it shall not be held responsible if a third party to which it transfers information uses it in a way contrary to any restriction.
4. Security. Organizations must take reasonable steps to protect individuals from loss, misuse and unauthorized access, disclosure, alteration, and destruction of personal information.

5. Data Integrity. Personal information must be relevant to the purposes for which it is to be used. Organizations should take reasonable steps to ensure that data is accurate, complete, current, and therefore reliable for its intended use.

6. Access. Individuals must have access to the information about them and be able to correct, amend, or delete information when it is inaccurate. An exception exists where the burden or expense of providing access would be disproportionate to the risks to the individual’s privacy in the case in question, or when providing access would violate the rights of persons other than the individual.

7. Enforcement. There must be a mechanism to assure compliance with the Principles that would provide recourse for individuals to whom the data relates affected by non-compliance. There must be consequences for an organization when it does not follow the Principles, including damages.

There is something pap-like about these Principles: a TV show written by a computer, a political program based upon public opinion polls. To a large extent they confirm what has been generally found acceptable. They tend to satisfy industry. They neither ruffle nor delight the consumer. They do not, of course, satisfy those committed to higher levels of privacy protection.

Commitment to the Principles may satisfy the United States Department of Commerce; this does not guarantee that they will satisfy the EU and the Directive’s requirements. Called “safe harbor,” the Principles do not contain the assurance that those words imply. Will one who adopts them be sure that they will satisfy the Directive and the EU may freely transfer information to the United States? As the Principles were working their way through the drafting process, there was considerable sentiment in both the United States and Europe that they did not go far enough to give the kind of consumer protection the Directive calls for.
To obtain a definitive ruling, the Principles’ efficacy was put to the Commission of the European Communities. The Commission decided that the Principles satisfied the Directive. The essence of the decision held that: “[t]he adequate level of protection for the transfer of data from the Community to the United States recognised by this Decision, should be attained if organisations comply with the Principles for the protection of personal data transferred from a Member State to the United States . . . .”

An additional problem, however, relating to the interrelationship of the Directive and the Commission Decision remains. The Decision provides that there shall be assurance that voluntary acquiescence in the Principles shall have teeth. Organizations shall “be subject to the jurisdiction of the Federal Trade Commission . . . or that of another body.” It further provides that for an organization in the United States to obtain the benefit of the Principles, the organization must be:

subject to the statutory powers of a government body in the United States listed in Annex VII to this Decision which is empowered to investigate complaints and to obtain relief against unfair or deceptive practices as well as redress for individuals, irrespective of their country of residence or nationality, in case of non-compliance with the Principles.

Two regulatory agencies are listed in Annex VII, the F.T.C. and the U.S. Department of Transportation. The latter Department is of fairly limited jurisdiction. By way of contrast, the F.T.C. has broad regulatory powers over most of the businesses in the United States. Unfortunately, banks are exempt from that regulatory reach and generally subject to the control of their specific financial regulators, both at the state and at the federal level. This leads to the conclusion that banks, some of

29. See John R. Schmertz & Mike Meier, Japan Issues Law Approving Electronic Signatures and Certification Services, Reflecting Efforts Underway in U.S. and EU to Provide Legal Effect to Such Transmissions, Int’l L. UPDATE, July 2000, available at LEXIS, Legal News, International Law Newsletters. We do not attempt here a reading of the jurisdiction of the Commission to decide this question. Suffice to say that it is apparently subject to some question.


31. We include here such organizations as the Federal Reserve Board, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation and, of course, the many state regulators that have primary jurisdiction over the state bank system.
the major disseminators and users of consumer personal finance information, cannot benefit from the Principles. It would consequently appear that American banks, barring some variation in law not now contemplated, are prohibited from receiving personal information from the European Community. As American banks now have major branches, affiliates, and subsidiaries in the EU, this can be a major business problem. (Where banks will land in this morass is open to question. A Department of Commerce spokesperson warned the banks that if they did not sign on to some form of protections, they would miss out on business opportunities in Europe).32

As of the beginning of October 2001, 103 companies in the United States had signed on to the Principles. This was up from 30 in May. Despite the more than 300 percent rise, only a minuscule portion of the millions of U.S. businesses seemed to experience sufficient desire for information from the EU and sufficient confidence in the Principles to join the system. Most of the signatories were little-known companies; some (Hewlett-Packard, Yamaha, B.M.W.) were not. It is presently unclear as to why the response was so stingy. Perhaps few companies believe that they have need of EU information; perhaps they believe that the Directive’s terms will not impede delivery; perhaps they believe that the Principles will really have no effect.

III. PRIVACY IN THE TWENTY-FIRST CENTURY

Consumer spokespeople are asserting that the disclosure of personal information has gone too far and that greater restraints upon the various dissemination systems are now appropriate. However much an individual may deplore the loss of personal privacy, the question is rarely asked: are we in a situation where it is still possible to restrain the outward flow of information, or has the technical capacity of contemporary computer equipment already outstripped that ability. There are some indications that

32. W.A. Lee, U.S. Banks Urged to Meet E.U. Data Rules, AMERICAN BANKER, Oct. 24, 2000, at 1. Ms. Wellbery, the then head of the electronic commerce task force for the International Trade Administration in the Department of Commerce and a primary draftsperson for the Principles, is now a lawyer in private practice in Washington, D.C. Id. See also Guy Jonquieres De, EU ‘No’ to Data Privacy Delay, FIN. TIMES, May 7, 2001, at 9. Meanwhile, the EU Commission seems to be undecided as to the approach it should take to the dilemma and is considering options. Id.
we may not yet have gone too far. A French court recently ordered Yahoo!, the U.S. based server, to take all possible measures to prevent France's access to web pages stored on Yahoo!'s server that auction Nazi objects, or present any Nazi sympathy or holocaust denial.33 The French court's ability to validly prevent a foreign sender electronic access to its territory has been interpreted as an indication that the world is under control. The Yahoo! case, however, represents but one instance of an immeasurable number of disclosure opportunities.

New generations of computer equipment are constantly outstripping their bounds. "If personal information exists on the Internet, it can be found by anyone who is interested enough to go looking for it... Each week, information becomes easier to obtain. This trend will continue for the foreseeable future."34 Equipment manufacturers still protest that their machines are subject to control; but their protestations have a hollow ring. In an article on computer sophistication and privacy, the New York Times concluded, "[t]hat quandary - that it is almost impossible to compartmentalize information for one purpose so that it cannot be misused - lies at the heart of the (privacy) argument."35 The manufacturers apparently do not realize that they have already lost the argument when they defend their products as privacy-friendly. The same article makes a more cogent comment when it quotes the CEO of Sun Microsystems: "You already have zero privacy - get over it."

In both the EU and the United States, it appears that the law of privacy is still essentially undefined. The system is out of control, and privacy is simply not protected regardless of Europeans' belief that their privacy is protected and Americans' express desire for privacy. Despite the arguments for and against privacy in the consumer and business communities and before the legislatures, it really is not an issue at all. I suggest that there is so much information out there about us that we can now afford to ignore it. (At least most of it. The end of this article briefly addresses areas where rights of privacy may still have some cogency.) It is like the naked man on the nude

34. Carole A. Lane, Naked in Cyberspace XXV (1997).
beach. His condition does not concern him as it would if he dropped his clothes in the lobby of the Waldorf.

The point is only gradually being made that those arguing for stronger privacy rights generally have little concept of what they have already lost, nor do they have a well-structured idea of how little that has meant to them. The dissemination of personal information does not require that information be formally sent for it to be received and electronically transcribed. Most of what is put on computers, particularly those connected to large business networks, is received and stored without the putative sender’s knowledge. Equipment that records, compiles, reconfigures, and even retransmits information has overwhelmed our ability to retain our privacy. Automobiles are increasingly sending information about where they are and how they are performing that is being stored and collated. This amorphous system has not been formally designed, nor has it been analyzed or diagrammed. “In this environment, it may be very difficult for individuals or organizations to be sure what information is being collected, to what uses that information is being put after it has been collected, or with whom the information is being shared.”

New York Times columnist Thomas L. Friedman wrote under an Accra, Ghana dateline:

If you're wondering why I came to Ghana, I can now reveal the truth: I came to check my health insurance. No, really. You see, I'm enrolled with Aetna health insurance. And Aetna, as well as Keystone, Mercy health care, has moved a large chunk of its data processing to a modern high-rise in downtown Accra. There 400 young Ghanaian techies - working in three eight-hour shifts and connected to the U.S. by satellite - punch the raw claims data sent to them by the U.S. health care giants onto computerized forms and then zip it back by satellite to the U.S. for final processing.

We have come close to creating a system beyond our control. Everything about us is out there, from our taste in automobiles to our sock size, in central data bases or aggregated by specialized service companies, often at the customer's specific request, but not necessarily so. As with Thomas Friedman’s in-

Insurance information, personal information is increasingly controlled by foreign technicians in foreign databases. It is all stored in contemporary computers and can be refined, subdivided, expanded, combined, and transported as needed. Limousines or SUVs, size 10, or medium?

The consumer is normally unaware of the tracks he or she is creating. A casual transaction will normally create multiple items of information. When we buy a train ticket or use an electronic toll pass, our travel routes are recorded as is the purchase form used. Payments lead to our bank accounts, while the use of credit notes our obligations and affects our creditworthiness. When we surf the Internet, our various interests are automatically recorded in different places; it is not necessary even to use a credit card or subscribe to a chat room to leave an individual’s spoor, although those connections create their own records. Even when we register objection to the collection of information, we are recorded as being in an identifiable group: those who are sensitive to the use of information. It is becoming too much to control.

A worldwide cease-and-desist order on the spread of information is probably not too late to impose. For such an order to be effective, however, it would take the cooperation of all countries, large and small, and require agreement as to what should be done. This is not impossible, but highly unlikely. Given the dissension already existing within privacy circles in the United States, we are not likely to reach international agreement on a desirable privacy policy. Whatever is done will be the result of broad compromise among groups in disagreement. To expect that such a compromise position can be achieved throughout the world requires at the very least a United Nations squared.

Of what value are the privacy protections already in place. This article later addresses the specialized fields that probably do require the concealment of individual information. Those are, however, few. What of the mass of consumer communication being logged every minute of every day. Is this really of significance to the consumers affected? If it is really useful to some, such as the people selling size 10 socks or SUVs, how much do the rest of us really care? What is the degree of importance to be given to the fact that I repaired my car at Steve & Francine’s on West 60th Street and bought a bus ticket to Binghamton? That information is already stored on various com-
puters in various ways and in various countries. What effort and
at what cost do we want to give to suppressing it?

Feelings matter. Most people probably do have some sense
that much about them is inviolate and should not be viewed by
others. “Americans treasure privacy” wrote Clinton and Gore
in 1995. If asked to write a similar document today, they would
probably say the same thing. To say to the multitudes that their
privacy is a myth and should simply be eliminated is a tall order.
Put that way, it would probably be rejected.

Our free enterprise system, backed up by a common law
legal system, often leaves an individual without an anchor.
Neither system results in conclusive answers. Cases in the
United States Supreme Court frequently have dissents, which
means that at the very highest level there is disagreement on
what the law is. Yet we more than survive; we frequently thrive.
Congress professes to believe in free enterprise. Yet, given a
problem, how few of our elected representatives will say “leave
it alone, the system will take care of it.” Whatever belief there
may be in free enterprise rarely manifests itself among legisla-
tors. That is what is happening to the privacy debate. If there is
a problem, let’s write a law.

One cannot advise a consumer public to forget its rights of
privacy, whatever they may be. One can more successfully point
out that those rights have been honored within the flexible
bounds of the free enterprise system to the public’s general sat-
sisfaction. We have been engaged in electronic trade for some
years now with a fairly good grip on our privacy rights. It is not
our function here to give the details of those protections. The
nature of our system, however, provides that our banks, for ex-
ample, have little in the way of specific restraints upon their use
of consumer information. Nevertheless, the banking system rec-
ognizes our expectation of privacy and honors it. Banks are ac-
tually restrained by reported cases that for years have been
balancing business’ rights in information collected against the
consumer’s need for privacy and developed a living doctrine
that has largely satisfied both. One doctrine not widely under-
stood, but of continuing value to both bank and customer, is the
common law doctrine of implied contract. It holds that when a
customer does business with a bank, they enter into a contract,
albeit implied in nature, that places certain limits upon the
bank’s use of the customer’s information. The limits are cloudy
and difficult to define. They do not satisfy those with need for precision in legal matters, but they work. 39

Subject to increased pressure to provide privacy protection - a protection already given - banks have begun to impose requirements upon their equipment vendors that exceed the warranties that the vendors can give. A recent article reports:

banks are beginning to go beyond the scope of the law to impose terms they (the vendors) find hard to meet . . . . In the new environment, financial services companies are asking to examine the security of all systems maintained by Unisys (an equipment vendor). The Blue Bell, Pa., company operates 4,000 server computers and 30,000 desktop PCs worldwide and each of them would be subject to individual scrutiny by each customer ‘whether or not it has anything to do with the problem at hand,’ Mr. Cawthorne (a Unisys VP) said. 40

The scope of the problem—if there is a problem—is too large for comprehensive management. Nevertheless, the nature of an individual’s personal information legitimately deemed private is generally kept private by the operation of the system. Banking is one example that is consistent with current economic theory. Our best protection as consumers is still considered to be the free market. Karl Marx sat for years in the British Museum and conceived a theory of a controlled economy that parsed logically; its problem was that it did not work. Almost all the old controlled states have broken under the relentless pressure of free enterprise. The consumer is protected from oligopoly pricing and restraints on output, not by wise men deciding upon the appropriate prices, but by open competition.

More information is conducive to more competition. Those who believe in the system of open, essentially unfettered competition should be opposed to greater financial privacy laws. The direction a new level of governmental restraint will lead can never be known for certain. Predictions that a particular alteration mandated by law in the current economic pattern will have certain results are usually wrong. The recent attempts to correct an economic slowdown through interest rate cuts are an example of this. The social structure today faces a grave risk from the growing reliance upon economics as a predictive device. We are experiencing this today in proposed changes to our bankruptcy

39. See Fischer, supra note 3, at ¶ 5.04[3]; Consumer Bankers Association, supra note 9.
laws. Changes are proposed by academics working in seclusion like Karl Marx in the British Museum, and telling us the effects of their proposals with unjustified self-confidence. Any prediction as to the effect of newly conceived privacy laws contains the same assumptions and the same risk of error.

The EU does not have the American confidence in the free market system. This difference in attitude may explain the contradictions noted above between EU law and EU practice. In the above-cited article, Professor Cate asserts that the relatively uncompetitive European financial system feeds off the restrictive privacy laws: “[e]fforts to open the financial services industry - to foster the development of competition, better serve customers, lower prices and compete more effectively with U.S. institutions - have largely failed because of restrictive privacy laws.”

Consumer groups and certain academics in the United States are lobbying Congress, the state legislatures, and bank regulators to impose further restraints upon the free flow of information. Basically, they do not believe the concept of the free market system and feel more confidence in a body of unyielding statutes and regulations, than in the relatively messy world of free enterprise. As a baseball manager will allow his pitcher to pitch out of trouble, our economy and our common law system effectively deal with troublesome issues by leaving them alone. Legislators cannot abide by free enterprise, but it works.

In the tradition of governmental control, we freeze development and evolution on the one hand; and do not accomplish anything on the other hand. For example, see how long it took the banking system to rid itself of Glass-Steagall constraints to the time when Congress was willing to acknowledge that it really had nothing to worry about. Bureaucratic solutions based upon notices, consents, and lists of regulatory rules look to the law of the past. They are reminiscent of exercises conducted under the Truth in Lending Act, Fair Credit Reporting Act, Delayed Funds Availability Act, and more. Tired notices to the


42. See generally CATE, supra note 24.

43. The 1934 Glass-Steagall constraints lasted from 1934 to 1999 when the Gramm-Leach-Bliley Act was enacted.
consumer in 10-point type led inexorably to the privacy notices under the Gramm-Leach-Bliley Act.\textsuperscript{44} The notices that were sent out, filled with legal jargon, neither informed nor pleased anyone. New conferences are under way to decide how to comply with the notice requirement. What had been a debate about privacy has turned into a different but more familiar debate about how new legal requirements can be met.

A largely unrestrained system of open information with the stimuli it gives to competition and business development is far preferable to the constipated world of privacy to which so many now aspire. Rather than a life largely blocked off from public view where invasions of privacy are narrow beams of light unexpectedly shone into a world of concealment, lives are becoming generally exposed. As it becomes increasingly difficult to conceal where we went, what we read, what we bought, what we played, and what we surfed for on the Internet, those subjects become less areas of secrecy than a vast illuminating sunlight. We need no longer fear that dictatorial power will use our shortcomings to bring us under its rule.\textsuperscript{45} Everyone is out there, and the new reaction to what used to be considered an invasion of privacy should be “so what.” Ironically, too much is becoming less.

What have been thought of as invasions of privacy are becoming more numerous. Our reaction should, however, not be to build more complex walls of protection. We are protected by the very invasions themselves. They should no longer even be called invasions of privacy. Fresh air is a better term.

\section*{IV. Conclusory Observations}

This article suggests that the current disposition favoring increased privacy protection rights needs rethinking. That is about as far as this article wants to go. Success will be measured by those who had previously taken privacy as an obvious good

\textsuperscript{44} Gramm-Leach-Bliley Act of 1999, supra note 16, at § 502. “[A] financial institution may not . . . disclose to a nonaffiliated third party and nonpublic personal information unless such financial institution provides or has provided to the consumer a notice . . . .” \textit{Id.}

\textsuperscript{45} See generally Admonition from the Health Information Privacy Rules Issued by the Department of Health and Human Services, 65 Fed. Reg. 82460 (Dec. 28, 2000). “[I]t is important not to lose sight of the inherent meaning of privacy: it speaks to our individual and collective freedom. \textit{Id.}
who will wonder whether they should not reconsider what they have been taking for granted. This article is not recommending legislative change. More accurately, it is suggesting that we refrain from change, at least until our priorities are properly ordered.

This is not to say, however, that privacy protections are uniformly useless. A substantial number of privacy protections are written into existing law and many of them are of great value and should, at the very least, be retained. In general, they result from the play of the free enterprise system and do not derive from an umbrella concept of privacy. Medical confidentiality heads the list. Certainly on the list are confidential communications with lawyers and confessions to the clergy. The common law gives us rights of privacy in our homes and while reading poetry in our gardens. There is no present need to tamper with these on any wholesale basis.

As to the general compulsion that our income and assets (including bank accounts) be kept confidential, the author is not sure what to say. He was well trained by his parents not to discuss money or sex and continues to abide by the advice. Perhaps this social norm should be examined. In any case, our bank records are now protected by a broad variety of state statutes and common law doctrines including the law of quasi-contract\textsuperscript{46} (protecting the level of privacy it is generally assumed that we want). Our current level of bank privacy is believed acceptable—or else there would have been a revolt or some massive change of banks before now.\textsuperscript{47}

Our present messy system of free enterprise, whose major tenet is that problems will work themselves out and should not be dealt with by legislatures or regulators, should be allowed to function. It should be supported by the equally unsatisfying system of the common law which, more often than not, does not even attempt to deal with problems as much as with particular conflicts and leaves the problems to work themselves out tomorrow. Today's law of privacy is a vast collection of federal and state constitutions, statutes, regulations, and common law

\textsuperscript{46} See generally \textsc{Fischer}, supra note 3.

\textsuperscript{47} With the free enterprise system in place, dissatisfaction with existing banks would have caused other, newer, banks to be created with the desired levels of privacy. That this has not happened is a prime source of belief that the existing system is acceptable.
principles that are there for the beleaguered consumer and his clever lawyer to use as needed. They are probably our best method for dealing with the difficult issue of privacy.