PROPOSED CYBERSPACE PRIVACY ACT

from *Information Privacy in Cyberspace Transactions*
50 STAN. L. REV. 1193-1294 (1998).

[footnote cross-references are not available]

A BILL[1]

To protect information privacy in cyberspace

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

Section 1. *Short Title.*

This Act may be cited as the "Cyberspace Privacy Act of ___."

Section 2. *Definitions.*

As used in this act—

(1) "Cyberspace" means any communication service or system that provides computer-mediated access through electronic communications to a computer server. "Cyberspace" explicitly includes, without limitation, any communication service or system that provides or enables electronic communications through the Internet.[2]

---

1. Those readers who conclude that this bill is too vague or radical might want to review the privacy provisions of the Cable Communications Policy Act of 1984, 47 U.S.C. § 551 (1988 & Supp. V 1993), and the Video Privacy Protection Act of 1988, 18 U.S.C. § 2710-2711 (1994).

2. I have not located any especially useful definition of cyberspace in federal or state legislation. The Communications Decency Act makes mention of an "interactive computer service," from which my definition borrows somewhat:

> The term 'interactive computer service' means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions.

47 U.S.C. § 230(e)(2) (1997).

The Consumer Internet Privacy Protection Act of 1997 also uses the term "interactive computer service," defined as "any information service that provides computer access to multiple users via modem to the Internet." H.R. 98, 105th Cong. § 4(1) (1997). The use of the word "modem" is problematic because, technically speaking, computers do not use modems, which change digital signals from the computer to analog signals carried over analog telephone networks, over fully digital communication networks.

Other attempts at regulating cyberspace have failed to produce crisper definitions. *See, e.g.*, N.Y. PENAL LAW § 235.21(3) (McKinney 1997) (defining a "computer communication system" as one "allowing the input, output, examination or transfer, of computer data or computer programs from one computer to another").

(2) "Electronic communications" has the same meaning as in 18 U.S.C. § 2510(12).[3]

(3) "Internet" means the globally distributed network of computers and telecommunications devices, owned both privately and publicly, that support communications through

(A) the Transmission Control Protocol/Internet Protocol ("TCP/IP") suite, or its subsequent extensions; or

(B) any protocols interoperable with the TCP/IP suite or with its subsequent extensions.[4]

(4) "Personal information" means information identifiable, directly or indirectly, to an individual, household, or to a specific computer regularly used by fewer than the same ten individuals. It includes, without

---

3. It means:

> [A]ny transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include—
>
> (A) any wire or oral communication;
>
> (B) any communication made through a tone-only paging device;
>
> (C) any communication from a tracking device (as defined in section 3117 of this title); or
>
> (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds;

18 U.S.C. § 2510(12) (1994). By excluding wire communications, the Cyberspace Privacy Act does not cover personal information collected through, for example, a traditional telephone conversation.

4. The California Business and Professional Code defines the Internet as:

> [T]he global information system that is logically linked together by a globally unique address space based on the Internet Protocol (IP), or its subsequent extensions; and is able to support communications using the Transmission Control Protocol/Internet Protocol (TCP/IP) suite, or its subsequent extensions, or other IP-compatible protocols; and provides, uses, or makes accessible, either publicly or privately, high level services layered on the communications and related infrastructure described herein.

CAL. BUS. & PROF. CODE § 17538(e)(6) (West 1997). My definition differs slightly because (1) the reference to "globally unique address space" is redundant with the specification of the TCP/IP protocol, and (2) the phrase "high level services," which might be a reference to the Open System Interconnection reference model of networks, is vague.

I also prefer my definition over the one that appears in the 1996 Telecommunications Act, which defines the Internet as "the international computer network of both Federal and non-Federal interoperable packet switched data networks." 47 U.S.C. § 230(e)(1) (1997); *see also* Consumer Internet Privacy Protection Act of 1997, H.R. 98, 105th Cong. § 4(2) (adopting the same definition of the Internet); Social Security On-line Protection Act of 1996, H.R. 1287, 105th Cong. § 4(2) (1997) (same); Encrypted Communications Privacy Act of 1997, S. 376, 105th Cong. § 2805(b)(4)(F) (1997) (same). First, the use of the term "packet switched" is unclear. I assume that term is meant to distinguish the Internet from "circuit switched" networks, such as our public telephone system. But what about "cell switched" networks, such as Switched Multimegabit Data Service ("SMDS") or Asynchronous Transfer Mode? *See* HORAK, *supra* note **Error! Bookmark not defined.**, at 223, 293-316 (discussing cell-switching, SMDS, and ATM). Second, this definition fails to capture the heart of the Internet, which is the TCP/IP protocol. Therefore, it includes entirely proprietary networks that are packet switched, but neither interoperable with TCP/IP nor publicly accessible.

limitation, information that identifies said individual, household, or computer as having requested, offered, leased, financed, rented, purchased, sold, or exchanged particular items or general kinds of information, services, or goods.[5]

(5) "Individual" means a natural human being, regardless of citizenship or residence status.

(6) "Cyberspace transaction" means an interaction with an individual through cyberspace for the purposes of satisfying, accepting, or completing an individual's request, offer, lease, financing, rental, purchase, sale, or exchange of information, services, or goods. A "cyberspace transaction" specifically includes the browsing of a World Wide Web page through the hypertext transfer protocol and its subsequent extensions, regardless of whether any money is exchanged. A "cyberspace transaction" specifically excludes any portion of an interaction that is a message from an individual to an individual in a noncommercial context, or to a publicly accessible forum.

(7) "Message" means an electronic communication—such as electronic mail and its subsequent extensions—whose content is authored or prepared by an individual with the intent that that content be delivered to some person.

---

5. Notice how I am not focusing solely on sensitive information, leaving nonsensitive information up for grabs. This is not only because drawing a sensitive/nonsensitive distinction is difficult, *see* FEDERAL RESERVE REPORT, *supra* note **Error! Bookmark not defined.**, at 14-15 (discussing the difficulty of defining "sensitive"), but also because advanced data mining makes this distinction far less important. It is a common mistake to think that the danger cyberspace poses to privacy is captured in any single bit of personal information. In fact, any such morsel of data is likely to be inconsequential. Instead, the true privacy threat arises from the systematic, detailed aggregation of otherwise trivial data that allows the construction of a telling personal profile. What seems nonsensitive in isolation becomes sensitive in aggregation. As the Supreme Court has recognized, in the context of criminal records:

> [T]he compilation of otherwise hard-to-obtain information alters the privacy interest implicated by disclosure of that information. Plainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information.

United States Dep't. of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 764 (1989). In *Reporters Committee*, the Supreme Court decided whether the release of FBI "rap sheets" constituted an invasion of privacy within the meaning of the privacy exemption of the Freedom of Information Act. *See id.*; *see also* 5 U.S.C. § 552(b)(7)(C) (1982). The Court recognized the synergistic risk posed to privacy by profiles compiled from public conviction information that would otherwise enjoy a practical obscurity. It noted the vast distinction "between scattered disclosure of the bits of information contained in a rap sheet and revelation of the rap sheet as a whole." *Reporters Committee*, 489 U.S. at 764; *see also* Steven A. Bercu, *Toward Universal Surveillance in an Information Age Economy: Can We Handle Treasury's New Police Technology?* , 34 JURIMETRICS J. 383, 400 & n.89 (1994) (describing a "mosaic theory" of information, where the whole is greater than the sum of the parts).

(8) "Person" means a nongovernmental individual, partnership, association, limited liability company, cooperative, joint-stock company, trust, or corporation.[6]

(9) "Noncommercial context" means a context in which the primary purpose of the interaction is not to exchange, or facilitate the exchange of, information, services, or goods for money or money's worth.

(10) "Publicly accessible forum" means any forum available through cyberspace, such as a Usenet newsgroup, listserv, chat room, Multi-User Domain, World Wide Web page, and their subsequent extensions whose audience is not or cannot be readily restricted by the individual sending the message.

(11) "Processing" means any combination of acquisition, disclosure, or use of personal information. The term "use" includes, but is not limited to, storage, organization, analysis, matching, consultation, and destruction.

(12) "Functionally necessary" describes personal information processing that is necessary to execute the cyberspace transaction in which the personal information is originally acquired. This is limited to information processing necessary for successful communication; payment and delivery; dispute resolution; warnings to the individual of any defect or danger; maintenance of cyberspace infrastructure; protection from fraud and abuse; adherence to governmental recordkeeping regulations; and transfer of business ownership.[7] It expressly excludes processing of personal information to target information, services, and goods on the basis of that personal information to the individual.

(13) "Consent" means an individual's fully informed assent manifested by an affirmative act in a written or an electronic communication.

(14) "Law enforcement agency" means any agency of the United States or of a state or political subdivision thereof, that is empowered by law to conduct investigations of, make arrests for, or prosecute criminal offenses.

---

6. I add "limited liability company" and "cooperative" to the definition of "person" in the Telecommunications Act of 1996. *See* 47 U.S.C. § 153(32) (1997). I also add "nongovernmental," since this Act is meant to apply only to the private sector. By this limitation, I do not mean to close off further discussion on whether such an Act should also apply to the public sector.

7. The VPPA includes in its definition of "ordinary course of business" both order fulfillment and request processing. *See* Video Privacy Protection Act of 1988, 18 U.S.C. § 2710(a)(2) (1994). But these terms, according to the legislative history, permit "marketing to their customers." S. REP. NO. 100-599, at 14 (1988), *reprinted in* 1988 U.S.C.C.A.N. 4342-1, 4342-12. Because I do not consider such marketing to be functionally necessary, the phrases "order fulfillment" and "request processing" are absent from my Act's definition.

Section 3. *Notice.*

(a) NOTICE REQUIRED—A person that acquires personal information in the course of executing, or facilitating the execution of, a cyberspace transaction[8] shall provide clear and conspicuous notice about:

(1) why personal information is being collected;

(2) to whom the personal information is expected to be disclosed;

(3) what the personal information is expected to be used for;

(4) what steps will be taken to protect the personal information;

(5) the consequences of providing or withholding the personal information; and

(6) any rights of redress.

(b) TIMING—

(1) Functionally Necessary Processing—For personal information processing that is functionally necessary to the cyberspace transaction, the person that acquires such personal information shall provide convenient and reasonable access to the notice required in Subsection (a) to the individual.

(2) Functionally Unnecessary Processing—For personal information processing that is not functionally necessary to the cyberspace transaction, the person that seeks to acquire such personal information shall provide notice to the individual before any such processing takes place.[9]

---

8. Note that the Act does not apply solely to communications providers or other transaction facilitators. One rationale for such a limitation might be that communications providers act as gatekeepers between the individual and all transacting parties and thus have direct access to the most telling data. A similar argument could be made about electronic payment providers. By regulating electronic communication service and cable service providers, the current ECPA and the privacy provisions of the 1984 Cable Act reflect this sensibility.

Unfortunately, regulating transaction facilitators alone ignores the reality that transacting parties do a substantial amount of data collection in cyberspace. And even if we substantially restrict transaction facilitators' ability to acquire, disclose, and use personal information, that would hardly prevent transacting parties—which include every site we browse and every firm from which we purchase a product—from collecting, mining, and sharing our personal data with others. As noted above, the costs of data exchange will continue to decrease in cyberspace due to advances in telecommunications technology and the standardization of data templates. Transacting parties will therefore be able to share databases with ease. As a long-term solution, it is naive to think that regulating transaction facilitators alone will adequately address cyberspace privacy concerns.

9. These provisions are constructed to avoid redundant or wasteful notices. For functionally necessary processing, individuals will likely—although admittedly not always—have a rough sense of how that information will be used, even without express notice. For these uses, therefore, an information collector need only make its privacy practices reasonably available. For example, when an individual gives her name and address to a pizza parlor through an e-mail, prior explicit notice would unduly burden the consummation of the transaction if the restaurant will only use that information to deliver the right pizza to the right address. On the other hand, if the pizza parlor uses the information in a manner not functionally necessary—for example, to sell lists of high-volume

Section 4. *Processing.*

(a) PRIMARY MARKET LIMITATION—In the course of executing, or facilitating the execution of, a cyberspace transaction, a person shall not process personal information in a manner functionally unnecessary to the transaction without the prior consent of the individual.

(b) SECONDARY MARKET LIMITATION—Without the prior consent of the individual, a person shall not process personal information originally acquired from a cyberspace transaction if the person has knowledge or reason to know that such processing is functionally unnecessary to that cyberspace transaction.

Section 5. *Access & Archiving.*

(a) ACCESS & CORRECTION—A person that acquires personal information in the course of executing, or facilitating the execution of, a cyberspace transaction shall provide, upon request of the individual, clarification of the notice provided pursuant to Section 3, Subsection (a), without fee, cost, or charge. Said person shall also provide to the individual access to that personal information in a reasonable time, place, and manner, without fee, cost, or charge. Said person shall also provide to the individual a reasonable opportunity to correct any error in such personal information, without fee, cost, or charge.

(b) DESTRUCTION OF RECORDS—A person that acquires personal information in the course of executing, or facilitating the execution of, a cyberspace transaction shall destroy that personal information when it is no longer functionally necessary to the cyberspace transaction, unless a pending request for the personal information exists under Section 6 or the individual has given consent to keep the information for a longer period.

Section 6. *Disclosure Exceptions.*

Notwithstanding any other section of this Act, it shall be lawful to disclose personal information acquired in the course of executing, or facilitating the execution of, a cyberspace transaction to:

(a) a law enforcement agency pursuant to a court order if, in the court proceeding relevant to such court order—

---

customers to health insurance companies—then express notice is warranted. *See* IITF PRINCIPLES, *supra* note **Error! Bookmark not defined.**, at 7; *cf.* James v. Ford Motor Credit Co., 638 F.2d 147, 150 (10th Cir. 1980) (concluding that too much information in a disclosure "result[s in] a piece of paper which appears to be 'just another legal document' instead of the simple, concise disclosure form Congress intended" (quoting S. REP. NO. 96-73, at 3 (1979), *reprinted in* 1980 U.S.C.C.A.N. 280, 281-82)).

(1) such agency offers clear and convincing evidence that the individual to whom the personal information pertains is reasonably suspected of engaging in criminal activity and that the personal information sought would be material evidence in the case; and

(2) the individual is afforded the opportunity to appear and contest such agency's claim.

(b) a law enforcement agency or a medical professional if such information is—

(1) critical to the life, healthy, or safety of the individual; and

(2) exigent circumstances preclude the possibility of obtaining consent from the individual.[10]

Section 7. *Relief & Enforcement.*

(a) CIVIL ACTION—Any individual aggrieved by the processing of his or her personal information by a person in violation of this Act may bring a civil action against that person in a United States district court without regard to the amount in controversy.

(1) The court may award actual damages but not less than liquidated damages computed at the rate of $100 for each separate violation or $5000, whichever is higher. The court may award reasonable attorneys' fees and litigation costs to the plaintiff if the plaintiff prevails. The court may also award punitive damages for purposeful violations of this Act made in exchange for valuable consideration.

(2) The remedies provided by this Section shall be in addition to any other lawful remedy available to the aggrieved individual.

(b) ADMINISTRATIVE ACTION—The Federal Trade Commission shall have the authority to investigate any act or practice to determine whether this Act has been violated. The Federal Trade Commission shall also have the authority to issue cease and desist orders to any person in violation of this Act, as if the person were in violation of section 5 of the Federal Trade Commission Act.

Section 8. *Statute of Limitations.*

No civil action shall be maintained under the provisions of this Act unless it is commenced within four years after the claim accrued.

---

10. *Cf.* An Act Respecting the Protection of Personal Information in the Private Sector, 1993 S.Q. 507 (Can.) (permitting disclosure "to a person to whom the information must be communicated by reason of the urgency of a situation that threatens the life, health or safety of the person concerned").

Section 9. *Preemption.*

No state or political subdivision thereof shall enact or enforce different statutes, regulations, or ordinances[11] concerning the processing of personal information acquired by a person in the course of executing, or facilitating the execution of, a cyberspace transaction.

11. I do not mean to preempt the common law tort of invasion of privacy.