Fordham Law Review

Volume 64 | Issue 3 Article 5

1995

Privacy and Security of Data

Judith Beth Prowda

Privacy and Security of Data

Cover Page Footnote

Research Fellow, Engelberg Center on Property and Innovation, New York University School of Law; Sarah Lawrence College (A.B.), Middlebury College (M.A., French Language and Literature), The Johns Hopkins University School of Advanced International Studies (M.A., International Relations), Fordham University School of Law (J.D.), New York University School of Law (L.L.M., Trade Regulation). The author wishes to thank Professor Rochelle Cooper Dreyfuss, New York University School of Law, and Professor Joel R. Reidenberg, Fordham University School of Law, for their valuable comments to earlier drafts of this section of the Report.

PRIVACY AND SECURITY OF DATA

*Judith Beth Prowda**

INTRODUCTION

The right to privacy was defined more than a century ago by Judge Thomas M. Cooley as the right "to be let alone."[210] In an oft-cited law review article written in that era, Samuel D. Warren and Louis D. Brandeis concluded that the right to privacy was based on a broader principle and claimed that the growing excesses of the press justified a remedy based on the infliction of mental distress upon private individuals.[211] Following this seminal piece, so many authors have written on the right to privacy that scholars on the subject have remarked that "no other tort has received such an outpouring of comment in advocacy of its bare existence."[212]

The right to privacy[213] is not expressly granted in the U.S. Constitution. Nevertheless, the Supreme Court has interpreted the Constitution to grant to individuals the right to privacy, based on the First Amendment's freedoms of expression and association,[214] the Fourth Amendment's protection of persons, places, papers, and effects against unreasonable searches and seizure,[215] the Fifth Amendment's privilege against self-incrimination and requirement of due process,[216]

---

* Research Fellow, Engelberg Center on Property and Innovation, New York University School of Law; Sarah Lawrence College (A.B.), Middlebury College (M.A., French Language and Literature), The Johns Hopkins University School of Advanced International Studies (M.A., International Relations), Fordham University School of Law (J.D.), New York University School of Law (L.L.M., Trade Regulation). The author wishes to thank Professor Rochelle Cooper Dreyfuss, New York University School of Law, and Professor Joel R. Reidenberg, Fordham University School of Law, for their valuable comments to earlier drafts of this section of the Report.

210. Thomas M. Cooley, The Law of Torts 29 (2d ed. 1888).

211. *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 213-14 (1890).

212. W. Page Keeton et al., Prosser and Keeton on the Law of Torts § 117, at 850 (5th ed. 1984).

213. This section of the Report addresses the right to privacy, or the right of individuals to control information held by others, not privacy in the context of Supreme Court decisions pertaining to abortion or other personal behavior of individuals. The right to privacy, as used in this section, refers to "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." Alan F. Westin, Privacy and Freedom 7 (1967).

214. Stanley v. Georgia, 394 U.S. 557, 564-66 (1969); NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 460-63 (1958).

215. Katz v. United States, 389 U.S. 347, 350-53 (1967) (establishing protection of persons under the Fourth Amendment); Olmstead v. United States, 277 U.S. 438, 478 (Brandeis, J., dissenting) (1928); Boyd v. United States, 116 U.S. 616, 627-30 (1886).

216. Mapp v. Ohio, 367 U.S. 643, 656-57 (1961) (noting that an unconstitutional seizure is tantamount to coerced self-incrimination).

penumbras of the Bill of Rights[217] and the Ninth Amendment,[218] and the Fourteenth Amendment's guarantee of ordered liberty.[219] Indeed, as one privacy scholar observed, the right to privacy "has almost as many meanings as Hydra had heads."[220] Certain privacy rights cases decided by the Supreme Court focus on the right of individuals to control their lives through highly personal decisions.[221] The common thread in these cases is "that each citizen has a right of autonomy—a right to decide how to live and to associate with others, free from all but the most carefully limited impingements by governmental authority."[222]

At least ten states have constitutions that expressly define personal privacy as a protected and fundamental right.[223] Numerous federal and state statutes also protect individuals from governmental misuse of personal information.[224] A few specialized federal statutes adopt fair information principles for specific industries in the private sector.[225] As a practical matter, however, beyond Fourth Amendment search and seizure standards, few restrictions on personal data collection are imposed.[226]

---

217. Griswold v. Connecticut, 381 U.S. 479, 484-85 (1965).

218. *Id.* at 488-91 (Goldberg, J., concurring).

219. Roe v. Wade, 410 U.S. 113, 152-53 (1973).

220. Diane Leenheer Zimmerman, *False Light Invasion of Privacy: The Light That Failed*, 64 N.Y.U. L. Rev. 364, 364 (1989). For a recent discussion of constitutional privacy, see Ellen Alderman & Caroline Kennedy, The Right to Privacy (1995).

221. *See, e.g.*, *Roe*, 410 U.S. at 152-53 (discussing a woman's right to abortion); *Griswold*, 381 U.S. at 485 (1965) (discussing the right of married persons to use contraceptives).

222. Zimmerman, *supra* note 220, at 364.

223. Raymond T. Nimmer, The Law of Computer Technology ¶ 16.08[2] (2d ed. 1992); *see, e.g.*, Ariz. Const. art. II, § 8 ("No person shall be disturbed in his private affairs, or his home invaded, without authority of law."); Cal. Const. art. I, § 1 (including privacy in a list of inalienable rights).

224. For example, two federal statutes bar private parties or the government from intercepting data. The Communications Act of 1934 prohibits any action to "intercept any radio communication and divulge [such communication]." 47 U.S.C. § 605(a) (1988). This law also applies to unauthorized access of an electronic database system. Telerate Sys., Inc. v. Caro, 689 F. Supp. 221, 230-31 (S.D.N.Y. 1988). The Electronic Communications Privacy Act of 1986 (the "ECPA") prohibits any unauthorized interception or disclosure of wire, oral, or electronic communications. 18 U.S.C. § 2511 (1994); *see infra* part II.F.3 (discussing the ECPA); *infra* part I.A (discussing the Privacy Act of 1974).

All states agree that certain records should remain confidential. Bruce D. Goldstein, Comment, *Confidentiality and Dissemination of Personal Information: An Examination of State Laws Governing Data Protection*, 41 Emory L.J. 1185, 1185 (1992). No two states, however, have adopted the same standards of confidentiality or procedural safeguards. *Id.* Some states omit entire categories of information, such as criminal, health, and tax records, from their confidentiality provisions. *Id.* at 1185 & n.3.

225. *See infra* part II. Most states have also enacted laws that apply to industry. Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?*, 44 Fed. Comm. L.J. 195, 227 & n.178 (1992).

226. Nimmer, *supra* note 223, ¶ 16.08[1]. In a landmark 1967 case, the Supreme Court held that the right to privacy found in the Fourth Amendment protects individ-

In recent years, the National Information Infrastructure ("NII"),[227] popularly known as the information superhighway, has expanded so rapidly that interactive technologies and integrated systems may eventually be widespread.[228] Modern technology allows students and researchers around the globe to browse through distant libraries and collaborate with others, by using a television, camcorder, only or personal computer.[229] In the near future, individuals may be able to join in family events or participate in electronic town meetings via the NII.[230]

Thousands of shoppers go online everyday for groceries, clothing, furniture, art work, or even a new home. The Internet, a "dense global matrix of 1.7 million computers,"[231] links fifteen to thirty million people in 137 countries and is steadily growing by a million users per month.[232] Commercial and noncommercial uses of the Internet are reportedly on the rise, making it "the world's most fashionable rendezvous."[233] In the private sector today, the dealing in personal information on individuals is a profitable industry. With the burgeoning of computers in the past decade, it has become easier than ever to build a detailed profile of an individual's behavior, political and sexual preference, social networking, driving record, and health status. This is done by simply gathering credit card data, telephone calling patterns, and other information available electronically.[234]

---

uals against warrantless wiretapping. Katz v. United States, 389 U.S. 347, 359 (1967). The Court established a standard for determining zones of privacy—whether the reasonable expectation of privacy outweighs the government's interest in conducting a search—based on the level of intrusion involved. *See id.* at 354-56. Thus, the Fourth Amendment protects not only an individual's tangible property, but also the individual's thoughts, communications, personality, and politics. In later cases, however, the *Katz* reasonable expectation of privacy standard was held not to be violated by certain intrusions because the circumstances of modern existence have diminished an individual's expectation of privacy. *See, e.g.*, Bowers v. Hardwick, 478 U.S. 186, 190-96 (1986) (upholding state anti-sodomy law as being rationally grounded in current moral views of Georgia citizens); United States v. Miller, 425 U.S. 435, 442-43 (1976) (noting lack of any legitimate expectation of privacy concerning banking records).

227. The NII refers to a "seamless interactive web of communications networks, computers, data bases, and consumer electronics" that will put vast amounts of information at the users' fingertips. Inquiry on Privacy Issues Relating to Private Sector Use of Telecommunications-Related Personal Information, 59 Fed. Reg. 6842 (1994) [hereinafter NTIA Notice of Inquiry].

228. Examples of interactive multimedia include participatory television, teleshopping, telebanking, video on demand, interactive video games, videoconferencing, remote medical testing and evaluation, and distance learning. Integrated digital technology permits an instantaneous dialogue between the user and system. Some of these technologies already exist and others exist in test stages. *See id.* at 6843-44.

229. *Id.* at 6844.

230. *Id.*

231. John Markoff, *The Internet*, N.Y. Times, Sept. 5, 1993, § 9, at 11.

232. *Id.*

233. *Id.*

234. *See* Reidenberg, *supra* note 225, at 197-98. In fact, credit card data represents only a small fraction of the information online, claims attorney Janlori Goldman of

According to some reports, over 10,000 lists of data about individuals are available for rent.[235] A recent estimate stated that the business of selling personal information was three billion dollars per year.[236] The estimated amount of time an average American professional will devote in a lifetime to sifting through direct mail solicitation is eight months.[237] One author, who posed as a CEO of a fictional direct mail corporation, discovered that 63.7 billion pieces of junk mail were sent from the companies he studied.[238]

Brokers and commercial services can readily provide consumer lists to the marketing industry, which boasts greater shopping convenience and better service for consumers.[239] Apparently, many American consumers agree. A spokesperson for Direct Marketing Association reported that "direct marketing accounts for $350 billion in sales annually, and 54% of adult Americans, or 111 million consumers, shop this way."[240]

Some consumers, however, may feel trapped in the web of target marketing.[241] Inevitably, a certain number of these consumers may also fall victim to computer error. While the exact number of errors is in dispute, one credit bureau in the New York City area found errors in 43% of their files.[242] That rate, projected to the nation's 400 million credit files, would mean that mistakes occur in roughly 172 million credit reports.[243] The nature of some of these errors is relatively minor, such as an outdated address.[244] Other errors, such as those confusing the credit information of two people with similar names, can

---

the ACLU's Privacy Project. Charles Piller, *Privacy in Peril: How Computers are Making Private Life a Thing of the Past*, The Recorder, July 19, 1993, at 8. Public records include information on real estate ownership, voter registration data, auto and driver records, and marriage records. *Id.*

235. Daniel Mendel-Black & Evelyn Richards, *Peering Into Private Lives*, Wash. Post, Jan. 20, 1991, at H1, H6; Jill Smolowe, *Read This!!!!!!!!*, Time, Nov. 26, 1990, at 62, 66 (referring to Standard Rate and Data Service publication of Direct Mail List Rate and Data, which describes over 10,000 commercially available lists); *see also* Deborah L. Jacobs, *They've Got Your Name. You've Got Their Junk*, N.Y. Times, Mar. 13, 1994, at 5 (noting that "[m]arketers can choose from among tens of thousands of lists" which can be rented or sold).

236. Smolowe, *supra* note 235, at 66.

237. *Id.* at 63.

238. Erik Larson, The Naked Consumer: How Our Private Lives Become Public Commodities 59 (1992).

239. Jacobs, *supra* note 235, at 5.

240. Thomas B. Rosenstiel, *Huge Databases, All Unregulated, Imperil Privacy*, Phila. Inquirer, May 21, 1994, at A2.

241. *See, e.g.*, Jacobs, *supra* note 235, at 5 (describing the "steady stream of unwanted mail" that consumers face). Some industries and organizations, however, such as J. Crew and the American Civil Liberties Union, give individuals the chance to "opt out by having their names withheld from lists." *Id.* The *New York Times* subscriber service offers this option to new and old subscribers. *Id.*

242. *What Price Privacy?*, Consumer Rep., May 1, 1991, at 356, 357 (describing Consolidated Information Service, a credit bureau in New York City).

243. *Id.*

244. *Id.*

have devastating effects.[245] Further, once a computer error is committed, correcting it can be a daunting task.[246]

Unbeknownst to most Americans, "personal data is [sic] being manipulated for purposes other than those originally intended when collected, and the parties engaging in such activities have no prior direct relationship with the individual about whom the information pertains."[247] In many instances, Americans would be shocked to learn how much of their lives are exposed to others.[248] People may face the possibility of discrimination by employers with access to sensitive information (e.g., prescriptions for medications for AIDS), or by insurance companies wishing to avoid customers having high-risk leisure activities (e.g., parachuting, scuba diving, or motorcycling).[249] Certain supermarkets electronically monitor purchases of customers, who participate in exchange for discounts.[250] Medical data are frequently circulated among insurance companies, drug companies, and marketers peddling myriad health care remedies and gadgets.[251] Undoubtedly, the information superhighway will accelerate this trend.

Recent polls indicate that Americans are extremely concerned about their privacy. According to a 1990 U.S. poll taken by Harris-Equifax, 90% of Americans believe that the collection of personal information is a problem.[252] Often information is gathered simply "because it's there."[253] The same poll found that 79% of Americans are concerned about their privacy and use of personal information, and believe that privacy ranks with "life, liberty, and the pursuit of happi-

245. For example, a couple from St. Louis, Missouri, had a bankruptcy filing inadvertently placed in their files. Banks cut off their loans and they eventually had to file for bankruptcy. Their suit failed because the law protects credit companies for "honest" mistakes. *Id.*

246. *Id.*

247. NTIA Notice of Inquiry, *supra* note 227, at 6842; *see also* Reidenberg, *supra* note 225, at 204-05 ("Information disclosed or collected for one purpose may easily have an associated use in an entirely different and undesirable context.").

248. Studies have indicated that if people realized how personal information can eventually be used, they might not have divulged it or entered into certain transactions requesting it. *See* Reidenberg, *supra* note 225, at 205-06.

249. Jacobs, *supra* note 235, at 5.

250. Reidenberg, *supra* note 225, at 203.

251. Larry Tye, *No Private Lives: Proposed 'Bill of Rights' Would Limit Personal Data*, Boston Globe, Sept. 8, 1993, at 1. For a discussion concerning the legal protection of the privacy of health care information and recommendations for reform, see Paul M. Schwartz, *The Protection of Privacy in Health Care Reform*, 48 Vand. L. Rev. 295 (1995).

252. *See* Reidenberg, *supra* note 225, at 203 (summarizing the results of a 1990 Harris-Equifax poll). The same poll found that 57% of Americans believe that consumers are asked to reveal excessive amounts of information. *Id.* at 203 n.37. Equifax, a leading credit agency, stopped selling credit information to direct marketers in 1991 as a result of its poll. *Consumer Credit Reports Get Special Attention*, A.B.A. Banking J., Mar. 1992, at 7, 9.

253. Reidenberg, *supra* note 225, at 203.

ness" as a fundamental right.[254] Almost three-quarters believe that they have lost control of the use and dissemination of personal information.[255] Many experts fear that George Orwell's *1984* could soon become a reality. Thus, it has become increasingly apparent that the current laws on information practices must be revised to ensure individuals the right to privacy in this electronic environment.

I. GOVERNMENT COLLECTION OF PERSONAL INFORMATION ON INDIVIDUALS

Congress has long grappled with the problems presented by the collection and dissemination of personal information concerning individuals through the development of sophisticated technologies. Congress realized that the federal government's use of computers to store and retrieve information about individuals increased the government's efficiency and effectiveness, but also threatened individual privacy.[256]

During the late 1960s and early 1970s, Congress held several hearings on privacy and the protection of sensitive personal information stored in computers.[257] In a Senate hearing during this period,[258] American legal scholar Arthur Miller detailed his concern for this trend and the alarming increase of the government's use of personal information that could be detrimental to individual privacy.

At one point, Congress considered the creation of a centralized data center containing information on all American citizens, such as Social Security numbers, income, and census data. Opposition, however, was vehement. The opposition voiced concerns that computers can be a method by which to achieve totalitarianism. The centralized data plan was tabled until the security and confidentiality of such information could be guaranteed.

---

254. *Id.* at 198-99 & n.14.

255. *Id.* at 199 n.14.

256. The legislative history of the Privacy Act of 1974 is collected in *Senate Comm. on Government Operations and Subcomm. on Government Information and Individual Rights of the House Comm. on Government Operations*, 94th Cong., 2d Sess., Legislative History of the Privacy Act of 1974, S. 3418 (Pub. L. No. 93-579): Source Book on Privacy (Joint Comm. Print 1976) [hereinafter Source Book].

257. *See, e.g., Federal Data Banks, Computers and the Bill of Rights: Hearings Before the Subcomm. on Constitutional Rights of the Senate Comm. on the Judiciary*, 92nd Cong., 1st Sess. (1971); *The Computer and Invasion of Privacy: Hearings Before the Special Subcomm. on Invasion of Privacy of the House Comm. on Government Operations*, 89th Cong., 2d Sess. (1966).

258. Professor Miller testified before the Senate in support of the Privacy Act in 1974. He stated:

> I think if one reads Orwell and Huxley carefully, one realizes that '1984' is a state of mind. In the past, dictatorships always have come with hobnailed boots and tanks and machineguns, but a dictatorship of dossiers, a dictatorship of data banks can be just as repressive, just as chilling and just as debilitating on our constitutional protections. I think it is this fear that presents the greatest challenge to Congress right now.

Source Book, *supra* note 256, at 160.

By 1973, the Watergate scandal had contributed to the growing public malaise and overall distrust of the government and its ability to probe into the personal affairs of individuals.[259] That year, the Department of Health, Education and Welfare ("HEW") proposed a Code of Fair Information Practices to be followed by federal agencies.[260]

A. *The Privacy Act of 1974*

In 1974, Congress passed the Privacy Act of 1974 ("Privacy Act"),[261] to "promote accountability, responsibility, legislative oversight, and open government with respect to the use of computer technology in the personal information systems and databanks of the Federal Government."[262] The Privacy Act of 1974 codified the following principles:

> (1) The privacy of an individual[263] is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies;
> (2) The increasing use of computers and sophisticated information technology, while essential to the efficient operations of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information;
> (3) The opportunities for an individual to secure employment, insurance, and credit, and his right to due process and other legal protections are endangered by the misuse of certain information systems;
> (4) The right to privacy is a personal and fundamental right protected by the Constitution of the United States; and
> (5) In order to protect the privacy of individuals identified in information systems maintained by Federal agencies, it is necessary and

259. *See* H.R. Rep. No. 1416, 93rd Cong., 2d Sess. 3 (1974).

260. U.S. Dep't of Health, Educ. and Welfare, Records, Computers and the Rights of Citizens xx-xxi (1973). The fundamental principles of the Code were: (1) there must be no personal data record-keeping systems whose very existence is secret; (2) there must be a way for individuals to find out what information is in their file and how the information is being used; (3) there must be a way for individuals to correct information in their records; (4) any organization creating, maintaining, using, or disseminating records of personally identifiable information must assure the reliability of the data for its intended use and must take precautions to prevent misuse; and (5) there must be a way for individuals to prevent personal information obtained for one purpose from being used for another purpose without consent. *Id.* This Code served not only as the framework for the Privacy Act of 1974, but also as the model for privacy legislation worldwide.

261. Pub. L. No. 93-579, 88 Stat. 1896 (current version codified at 5 U.S.C. § 552a (1994)).

262. S. Rep. No. 1183, 93rd Cong., 2d Sess. 1 (1974).

263. The Privacy Act defines an "individual" as "a citizen of the United States or an alien lawfully admitted for permanent residence." 5 U.S.C. § 552a(a)(2) (1994).

> proper for the Congress to regulate the collection, maintenance, use, and dissemination of information by such agencies.[264]

These principles were to serve as an " 'Information Bill of Rights' for citizens and a 'Code of Fair Information Practices' for federal agencies."[265] For example, with certain exceptions, the Privacy Act prohibits government agencies from disclosing any record on any individual for any purpose other than that originally intended without that individual's consent.[266] The Privacy Act also grants individuals a right of access to their records and the opportunity to amend their records based on a showing of a lack of accuracy, relevancy, timeliness, or completion.[267] To enforce certain provisions, individuals may bring a civil action against the agency for damages or injunctive relief, based on a showing of harm resulting from a government agency's intentional or willful act.[268] Individual officers or employees of agencies can also be subject to criminal sanctions under certain circumstances.[269]

In 1977, the United States Privacy Protection Study Commission published a report[270] assessing the effectiveness of the Privacy Act. The Commission's report concluded that the Privacy Act "has not resulted in the general benefits to the public" and "ignores . . . some personal-data record-keeping policy issues of major importance now and for the future."[271] To remedy these deficiencies, the Commission proposed that the Privacy Act be revised to clarify "the ambiguous language,"[272] provide individuals with broader remedies, and limit the "routine-use" exemption.[273]

In 1988, the Privacy Act was amended by the Computer Matching and Privacy Protection Act of 1988 ("Matching Act").[274] The purpose of the amendment was to regulate the use of data-matching procedures in federal agencies. This law, which regulates the matching of government files on individuals, such as lists of welfare recipients and interagency payroll records, has generated much debate in the area of privacy.[275] From the government's perspective, data matching is a

---

264. *Id.* § 552a.

265. Jerry Berman & Janlori Goldman, Benton Foundation Project on Communications & Information Policy Options, A Federal Right of Information Privacy: The Need for Reform 13 (1989) [hereinafter Benton Foundation Report].

266. 5 U.S.C. § 522a(b) (1994).

267. *Id.* § 522a(d)(2)(B)(i).

268. *Id.* § 522a(g).

269. *Id.* § 522a(i).

270. U.S. Privacy Protection Study Commission, Personal Privacy in an Information Society (1977).

271. *Id.* at 502-03.

272. *Id.* at 503.

273. *Id.* at 515-21.

274. Pub. L. No. 100-503, 102 Stat. 2507-14 (codified at 5 U.S.C. § 552a (1994)).

275. *See* Nimmer, *supra* note 223, ¶ 16.09, at 16-28.

cost-efficient way to allocate public resources[276] and detect waste, fraud, and abuse of government programs.[277]

Privacy advocates, however, view data matching as a form of "unnecessary incursion into privacy interests."[278] While the Matching Act did not limit the types of records that could be matched, it set forth a procedural framework requiring more adequate notice to individuals of the right to a hearing before benefits are cut off or denied, and mandatory reporting requirements for government agencies that match records.[279]

B. *Criticisms of the Privacy Act of 1974 and Proposals for Change*

In recent years, there has been a growing sentiment that the Privacy Act has failed to address new privacy concerns resulting from the increasing use of computerized records. For example, in a 1986 report, the Office of Technology Assessment ("OTA") reported that federal and institutional use of new electronic technologies in processing, comparing, and linking personal information has eroded the protections of the Privacy Act.[280] Two experts from the American Civil Liberties Union ("ACLU"), a privacy watchdog, criticized the Privacy Act for falling far short of achieving its initial objectives. They argued that the Privacy Act was "at best serving as a procedural hoop-jump for federal agencies,"[281] and charged government agencies with escalating, rather than limiting, the government's collection and dissemination of personal information.[282] In their view, Congress has failed to control the widespread misuse of an individual's Social Security number, not only by authorizing its use,[283] but mandating it.[284] For example, a 1986 Tax Reform Act provision requires that all children over five years of age who are claimed as dependents be assigned a Social Security number.[285]

---

276. *Id.*

277. Benton Foundation Report, *supra* note 265, at 14.

278. Nimmer, *supra* note 223, ¶ 16.09, at 16-28. For an insightful discussion concerning the problems associated with computer matching programs, see Kenneth J. Langan, *Computer Matching Programs: A Threat to Privacy?*, 15 Colum. J.L. & Soc. Probs. 143 (1979).

279. The Computer Matching and Privacy Protection Act of 1988, 5 U.S.C. § 552a(p)(1) (1994).

280. *See* Benton Foundation Report, *supra* note 265, at 2, 30 n.7.

281. *Id.* at 14.

282. *Id.*

283. *Id.* at 16; *see also* Letter from Electronic Frontier Foundation to Working Group on Privacy 7 (July 6, 1994) [hereinafter EFF Letter] (on file with the *Fordham Law Review*). The 1976 Tax Reform Act authorized states to use Social Security numbers for state or local tax purposes, welfare systems, driver's license systems, and locating parents delinquent in court-imposed child support payments. *Id.* (citation omitted).

284. Benton Foundation Report, *supra* note 265, at 16.

285. *Id.* (citing Tax Reform Act of 1986, 26 U.S.C. § 6109(e) (1988)); *see also* EFF Letter, *supra* note 283, at 7.

The Clinton Administration created a federal interagency task force in September 1993, called the Information Infrastructure Task Force ("IITF"), to work with Congress and the private sector on ways to advance the NII.[286] The IITF set up the Working Group on Privacy ("Working Group")[287] to investigate ways to balance society's need for the flow of information and the privacy interests of individuals.[288]

In May 1994, the Working Group published a set of principles addressing two major changes in information technology in the past two decades: the emergence of large privately-held databases and the development of interactive technologies.[289] The Working Group Draft, which requested public comment by June 1994, identified certain principles associated with the deterioration of privacy in the United States. These principles are discussed below.

1. General Principles for the NII—"Reasonable Expectation of Privacy" and "Information Integrity"

The Working Group Draft recommended that, to the extent reasonable, users of the NII "[e]nsure that information is secure, using whatever means are appropriate."[290] The Electronic Frontier Foundation ("EFF"),[291] a group commenting on the Working Group Draft principles, pointed out the difficulty in determining and applying a "reasonable expectation of privacy standard."[292] This is especially true in an interactive electronic environment where many levels of users participate in the exchange of information. The EFF believes that such a reasonableness standard "will depend on the legal and regulatory protections set by Congress and the agencies."[293] It recommended that the IITF draft a new legal definition of reasonable expectation of privacy that entails "an objective expectation of privacy protection, irrespective of the technological capability to intrude."[294]

286. The National Information Infrastructure: Agenda for Action, 58 Fed. Reg. 49,025, 49,035 (1993) [hereinafter NTIA Agenda for Action].

287. The Working Group on Privacy was set up by the Information Policy Committee of the IITF. This Working Group proposes to update the Code of Fair Information Practices developed by the HEW, the framework for the Privacy Act of 1974. Draft Principles for Providing and Using Personal Information, 59 Fed. Reg. 27,206 (1994) (proposed May 25, 1994) [hereinafter Working Group Draft]

288. *See* NTIA Agenda for Action, *supra* note 286, at 49,035.

289. Working Group Draft, *supra* note 287, at 27,206. Another set of Draft Principles was issued on January 20, 1995. *See* National Information Infrastructure; Draft Principles for Providing and Using Personal Information and Commentary, 60 Fed. Reg. 4362 (1995) (proposed Jan. 20, 1995). Comments were due by March 21, 1995. *Id.*

290. Working Group Draft, *supra* note 287, at 27,206.

291. The EFF, formed in July 1990, is a nonprofit public interest group, "dedicated to preserving and enhancing civil liberties in digital media. . . focus[ing] on privacy issues in the new electronic age." EFF Letter, *supra* note 283, at 1.

292. *Id.* at 4-5.

293. *Id.* at 5.

294. *Id.* at 6.

2. Principles for Information Collectors[295]

The Working Group Draft recommended that information collectors inform individuals of the purpose for which the information is being collected, its expected use, its protection in terms of confidentiality and integrity, the repercussions of providing or withholding information, and rights of redress.[296] The EFF suggested that the " 'routine use' exemption . . . clarif[y] that disclosure for a routine use must be *consistent* with the original purpose for which the information was originally collected."[297] Individuals must have the right to challenge any inconsistency with the proposed routine use and original purpose of the collection.[298] Further, routine uses, in the opinion of the EFF, should be "benign and not for the purpose of taking adverse action against an individual."[299]

3. Principles for Information Users[300]

The Working Group Draft recommended allowing "individuals to limit the use of their personal information if the intended use is incompatible with the original purpose for which it was collected, unless that use is authorized by law."[301] As noted above, Congress not only allows, but mandates the use of Social Security numbers at certain times. The EFF proposed limiting the authority of government agencies "to collect only information necessary and relevant to their particular purpose," and requiring the agencies to inform individuals of the reasons for collection and the purposes for which it will be used.[302]

a. *Fairness Principles*

The Working Group Draft also provided that users of information offer individuals "a reasonable means to obtain, review, and correct their own information."[303] Additionally, the draft proposed that individuals be provided the opportunity "to correct inaccurate information [if the inaccuracy] could harm them."[304] Because it is critical for

295. The Working Group defines information collectors as "entities that collect personal information directly from the individual." Working Group Draft, *supra* note 287, at 27,206.

296. *Id.*

297. EFF Letter, *supra* note 283, at 6-7. The authors of the Benton Foundation Report, a director and a staff attorney of the ACLU, share this view. *See* Benton Foundation Report, *supra* note 265, at 24.

298. EFF Letter, *supra* note 283, at 7.

299. *Id.*

300. The Working Group defines information users as "[c]ollectors and entities that obtain, process, send or store personal information." Working Group Draft, *supra* note 287, at 27,207.

301. *Id.*

302. EFF Letter, *supra* note 283, at 7-8.

303. Working Group Draft, *supra* note 287, at 27,207.

304. *Id.* In 1977, the Privacy Commission did not suggest changes to the original language in the Privacy Act regarding the accuracy of records. Individuals thus have

individuals to correct inaccurate information to prevent the propagation of errors, the EFF recommended that "users and collectors of information should develop technical mechanisms to detect, locate, and fix problems and correct errors."[305] In the EFF's view, "the right to correct [inaccurate] information should be incorporated into the design of all information systems."[306]

b. *Acquisition and Use Principles*

The Working Group recommended that "users of personal information should . . . [o]btain and keep only information that could reasonably be expected to support current or planned activities and use the information only for those or compatible purposes."[307] Further, the Working Group Draft stated that "[i]nformation users should . . . [a]llow individuals to limit the use of their personal information if the intended use is incompatible with the original purpose for which it was collected."[308] As some commentators have noted, the "routine use" exemption has been used to thwart the government's interpretation of "compatible" use.[309]

c. *Redress Principles*

The Working Group proposed that the right to redress should depend on the ability of an individual to show harm "resulting from inaccurate or improperly used personal information."[310] In some cases, however, adverse claims go unnoticed, and "redress will not be available."[311] The Working Group further commented that "individuals should be able to obtain from data users . . . a copy of this personal information and have the opportunity to correct inaccurate information."[312]

The EFF reported that in reality, however, "it is extremely difficult for individuals to obtain relief under the . . . Privacy Act," even if actual harm occurs.[313] A plaintiff must prove that the government acted intentionally and willfully.[314] This "one sidedness" in favor of the government record keeper is described as "one of the most ugly faces

---

no opportunity to correct inaccurate information. *See* 5 U.S.C. § 552a(e)(1), (5) (1994).

305. EFF Letter, *supra* note 283, at 9 (citation omitted).

306. *Id.*

307. Working Group Draft, *supra* note 287, at 27,207.

308. *Id.*

309. *See* Benton Foundation Report, *supra* note 265, at 14; EFF Letter, *supra* note 283, at 6-7.

310. *See* Working Group Draft, *supra* note 287, at 27,207.

311. *Id.* at 27,209.

312. *Id.* at 27,211.

313. EFF Letter, *supra* note 283, at 8.

314. 5 U.S.C. § 552a(g)(4) (1994).

of privacy."[315] Moreover, as one scholar has noted, "unless an agency is cooperative, the procedures for review can be time-consuming and expensive."[316]

To remedy these shortcomings, the EFF proposed a new section that provides both liquidated damages and injunctive relief for harms, including intangible harms, without requiring a showing of an adverse effect to the plaintiff.[317] Further, the EFF recommended that individuals "be informed of any actions taken as a result of incorrect information."[318]

4. Principles for Providing and Using Information

The Preamble of the Working Group Draft recited that "new principles [emerging as a result of the NII] must acknowledge that all members of our society (government, industry, and individual citizens), share responsibility for ensuring the fair treatment of individuals in the use of personal information."[319] Likewise, these individuals have a responsibility to obtain "adequate, relevant information" on: uses (primary and secondary) of the information;[320] efforts to protect the integrity and confidentiality of the information;[321] consequences for providing or withholding information;[322] and rights of redress.[323] The EFF believes that the ultimate responsibility for maintaining fair information should be placed on the collectors and users of information, not on the individuals who disclose the information.[324]

II. Private Collection of Information on Individuals

The collection of data on individuals by institutions in the private sector can also threaten the privacy interests of individuals. Private institutions, such as banks, credit card companies, and insurance companies, have the capacity to collect vast amounts of information about individuals,[325] which can be highly intrusive into their private lives. Furthermore, once such information has been collected and stored in computer systems, it can be analyzed and made available to secondary users "in the form of mailing lists and other information products."[326]

315. EFF Letter, *supra* note 283, at 8 (quoting Willis H. Ware, *The New Faces of Privacy*, 9 Info. Soc'y 195, 203 (1993)).
316. Nimmer, *supra* note 223, ¶ 16.08[3].
317. EFF Letter, *supra* note 283, at 8.
318. *Id.*
319. Working Group Draft, *supra* note 287, at 27,206.
320. *Id.* at 27,207.
321. *Id.*
322. *Id.*
323. *Id.*; *see also id.* at 27,210 (expanding on the awareness principles which allow the individual to make informed decisions about the information that they disclose).
324. EFF Letter, *supra* note 283, at 10.
325. Nimmer, *supra* note 223, ¶ 16.17.
326. *Id.*

Some uses of this information may merely be annoying, but others are more serious.

On the other hand, some Americans argue that consumers may actually benefit from wide dissemination of personal information. For example, they claim that the liberal exchange of financial data facilitates the provision of credit to consumers and enables creditors to charge lower interest rates to reliable debtors.[327] Retailers and marketers argue that by targeting their audience, they conserve paper, drive down prices, and increase consumer choice.[328] Mail-order shopping may be convenient and even essential for people with small children, physical disability, or little time to shop.[329] The environmentally conscious claim that mail-order shopping saves on gas and reduces traffic congestion.[330] Because wide dissemination of personal information may be beneficial, annoying, or harmful, determining who owns and has the right to control information on individuals is crucial.

At the present time, there is no omnibus privacy legislation applicable to the private sector in the United States.[331] In 1993, Senator Paul Simon (D-Ill.), proposed legislation that would create a Privacy Protection Commission.[332] This five-member independent commission would issue advisory opinions on the use and dissemination of personal information, investigate alleged abuses in publicly and privately maintained data bases, and oversee telecommunications and electronic privacy disputes and related security issues.[333] The Commission would not have enforcement powers.[334] This bill has stalled in Congress several times. The federal legislation that exists today has developed in an ad hoc manner, focusing on the privacy issues of specific industries.

---

327. *See* Steven A. Bibas, *A Contractual Approach to Data Privacy*, 17 Harv. J.L. & Pub. Pol'y 591, 598-99 (1994) (citing several arguments in favor of the uninhibited flow of information).

328. Daniel Klein & Jason Richner, *In Defense of that Pesky Junk Mail*, Chi. Trib., Apr. 20, 1992, § 1, at 19.

329. *Id.*

330. *Id.*

331. *See* Reidenberg, *supra* note 225, at 201. In contrast, several European nations have adopted omnibus legislation governing private sector data processing. *Id.* The European Community issued a draft directive on September 13, 1990. In addition, in February, 1995, the European Community approved a data protection measure that attempted to standardize existing national laws on the use of information gathered by states and governments. A new directive was pending approval by the European Parliament in the summer of 1995. Further, two important international organizations, the Organization for Economic Cooperation and Development and the Council of Europe, have set forth principles for information processing in the private sector. *See id.* at 200-01; Robert G. Boehmer & Todd S. Palmer, *The 1992 E.C. Data Protection Proposal: An Examination of Its Implications for U.S. Business and U.S. Privacy Law*, 31 Am. Bus. L.J. 265 (1993).

332. S. 1735, 103d Cong., 1st Sess. §§ 3-4 (1993); *see* 139 Cong. Rec. S16433, S16493-94 (1993).

333. S. 1735, 103d Cong., 1st Sess. § 6 (1993).

334. *See id.* § 8.

A. *Financial Data*

One area frequently litigated in the private sector falls under the Fair Credit Reporting Act ("FCRA"),[335] which Congress passed in 1970. This law regulates the disclosure of personal information by credit reporting agencies, but not the collection of such information. Under the FCRA, consumers may review their own records and correct inaccuracies. Information-collecting agencies may only disclose such information pursuant to a consumer's written instruction, a court order, or for certain enumerated purposes.[336] These agencies, however, are not required to notify individuals of the existence, content, or use of such records. Thus, as a practical matter, individuals may have difficulty enforcing their rights under the FCRA.[337]

Another law that affects credit activities and the use of personal information is the Fair Credit Billing Act of 1974,[338] which requires that consumers receive copies of consumer credit transaction records and have the right to correct inaccuracies.[339] Creditors are prohibited from disclosing information about late payments pending error resolution, but are not otherwise restricted from disclosing transaction records to third parties. Likewise, the Fair Debt Collection Practices Act of 1977[340] restricts communication to third parties of a debtor's financial status to information regarding the collection.[341] The Equal Credit Opportunity Act of 1974[342] prohibits dissemination regarding any aspect of credit on the basis of race, color, religion, national origin, sex, marital status, or age.[343] This law entitles individual applicants to a "statement of reasons" for denial of credit.[344]

The Electronic Fund Transfer Act of 1978 ("EFTA")[345] sets forth mandatory guidelines governing the use of electronic systems to transfer funds.[346] For example, EFTA requires detailed documentation of transaction data, such as the amount, date, and location of each trans-

335. 15 U.S.C. § 1681 (1994).

336. These purposes include extension of credit, review or collection of an account, employment, underwriting insurance, determination of eligibility for government benefits, and any legitimate business need in connection with a transaction involving the consumer. 15 U.S.C. § 1681b (1994).

337. *See* Reidenberg, *supra* note 225, at 211-12. Once the information is disseminated in accordance with the statute, the recipient will not necessarily be restricted from further circulating the information without the individual's consent. In certain circumstances, however, a secondary user of information may be considered a credit reporting agency and thus subject to the FCRA's disclosure restrictions. *See* 15 U.S.C. § 1681a(f) (1994).

338. *Id.* § 1666.

339. *See id.* § 1666(a).

340. *Id.* § 1692.

341. *Id.* § 1692c(b).

342. *Id.* § 1691.

343. *Id.* § 1691(a)(1).

344. *Id.* § 1691(d)(2).

345. *Id.* § 1693.

346. *Id.* § 1693(b).

fer, and requires financial institutions to provide consumers with periodic statements. EFTA has mandatory error resolution procedures. The EFTA, however, does not restrict the disclosure of transaction information to third parties or the duration information may be stored.

In 1978, Congress passed the Right to Financial Privacy Act,[347] which set forth procedural restrictions on the access of federal agencies to data held by a depository institution.[348] Congress enacted the Privacy Protection Act[349] in 1980 to prohibit government searches of press offices without a warrant if there is no suspicion of criminal activity.[350] In 1982, Congress granted individuals due process protection before the release of any federal debt information to a private credit bureau.[351] The Tax Equity and Fiscal Responsibility Act of 1982[352] restricts the disclosure of tax return information for purposes unrelated to tax administration.[353] This law authorizes disclosure of tax return information to law enforcement agencies to combat organized crime, narcotics trafficking, and other non-tax crimes.[354]

B. *Solicitations*

The Deceptive Mailings Prevention Act[355] bans mail solicitations that look like government notices[356] and prey upon the elderly and others, such as expectant mothers, who need to apply for Social Security cards. This law empowers the United States Postal Service to stop delivery of a mail solicitation that may reasonably mislead the public into believing that it was sent by the government or is government approved.[357]

To address telemarketing concerns, Congress passed the Telephone Consumer Protection Act[358] in 1991, permitting the Federal Communications Commission ("FCC") to designate an entity (in the usual case, the entity will be a company) to maintain "do not call" lists and

347. 12 U.S.C. § 3401 (1994). The Right to Financial Privacy Act was passed to overturn the Supreme Court decision, United States v. Miller, 425 U.S. 435 (1976). In *Miller*, the Court held that an individual had no enforceable expectation of privacy for records held by the bank. *Id.* at 441-43. Thus, the bank had a right to turn over data without the customer's knowledge to a grand jury in response to a subpoena. *See id.*

348. 12 U.S.C. § 3402 (1994).

349. 42 U.S.C. § 2000aa (1988).

350. *Id.*

351. 31 U.S.C. § 3716(a) (1988).

352. Tax Equity and Fiscal Responsibility Act of 1982, Pub. L. No. 97-248, 96 Stat. 324 (codified as amended in scattered sections of 26 U.S.C.).

353. 26 U.S.C. § 6103 (1988 & Supp. V 1993).

354. *Id.* § 6103(i)(1)(A).

355. Deceptive Mailings Prevention Act of 1990, Pub. L. No. 101-524, 104 Stat. 2301 (codified as amended in scattered sections of 39 U.S.C.)

356. *See* 39 U.S.C. § 3001(h) (Supp. V 1993).

357. *Id.*

358. Telephone Consumer Protection Act of 1991, Pub. L. No. 102-243, 105 Stat. 2394 (codified as amended in scattered sections of 47 U.S.C.).

honor consumer requests to be added to those lists.[359] This law, which amends the Communications Act of 1934,[360] directs the FCC to regulate telephone solicitations.[361] It is frequently described as a privacy law, but it really regulates nuisance calls employing pre-recorded messages or automatic dialing equipment.

C. *Education Data*

The Family Educational Rights and Privacy Act (the "Education Rights Act")[362] was passed in 1974 to regulate the disclosure of and access to educational records.[363] This law allows students to review their records and prohibits educational institutions from disclosing the content of a student's file, except in limited circumstances.[364] Federal funding of educational institutions may be terminated for noncompliance.[365] The Education Rights Act does not provide for a private cause of action for an affected individual.[366]

D. *Driver's Records*

The Driver's Privacy Protection Act of 1994[367] was passed in October 1994, making it a crime for state motor vehicle offices to release certain information about a licensee without a legitimate purpose. Under this law, individual states have three years to prepare regulations that will allow drivers to opt out of having personal information released, such as age and address.[368]

---

359. 47 U.S.C. § 227(c)(3) (Supp. V 1993).

360. 47 U.S.C. § 151-613 (1988 & Supp. V 1993).

361. *See id.* § 151.

362. Family Educational Rights and Privacy Act of 1974, Pub. L. No. 93-380, 88 Stat. 571 (codified as amended in scattered sections of 47 U.S.C.). This law pertains to schools that are federally funded and does not require the school to protect against the dissemination of student information through non-school sources. Frasca v. Andrews, 463 F. Supp. 1043, 1050 (E.D.N.Y. 1979). *But see* Fay v. South Colonie Cent. Sch. Dist., 802 F.2d 21, 33 (2d Cir. 1986) (holding that this Act, used in conjunction with other federal statutes, allows for private causes of action).

363. *See* 20 U.S.C. § 1232g (1994).

364. For example, educational institutions may disclose information contained in student records to student officials who need to know, research organizations, government officials, and people with enforcement subpoenas. *Id.* § 1232g(b). "Parents are permitted access to [an] institution's file, except [to view] confidential letters of recommendation and personal financial statements of college students." Nimmer, *supra* note 223, ¶ 16.19.

365. 20 U.S.C. § 1232g(f) (1994).

366. *Fay*, 802 F.2d at 33; Girardier v. Webster College, 563 F.2d 1267, 1276-77 (8th Cir. 1977); Smith v. Duquesne Univ., 612 F. Supp. 72, 80 (W.D. Pa. 1985), *aff'd*, 787 F.2d 583 (3d Cir. 1986).

367. 18 U.S.C. § 2721 (1994).

368. *See id.* § 2721(b)(11)-(12).

E. *Health Care Data*

The processing and use of health care information "plays a critical role in the provision, regulation, and financing of medical services by government and private entities."[369] Information is no longer exclusively in the hands of health care providers but is increasingly shared among a wide variety of entities as well.[370] There has been no noticeable change in the legal scheme since the Privacy Protection Study Commission completed its study almost twenty years ago.[371] One recent Office of Technology Report concluded that: "The present legal scheme does not provide consistent, comprehensive protection for privacy in health care information, whether it exists in a paper or computerized environment."[372] Indeed, one government policy analyst noted that "video rental records are afforded more privacy protection than are medical records."[373]

There are a few federal statutes, other than the Privacy Act of 1974, that govern the use of medical data. For example, federal alcohol and drug treatment statutes, with certain exceptions, prohibit the disclosure of an individual's participation in a rehabilitation program, without that individual's prior consent.[374] Aside from these laws, however, federal laws that restrict the use of health data once it has been obtained, have proven largely ineffective.[375]

---

369. Schwartz, *supra* note 251, at 300. For an analysis of international developments concerning the protection of medical data, see *id.* at 324-33; Spiros Simitis, *Reviewing Privacy in an Information Society*, 135 U. Pa. L. Rev. 707 (1987).

370. *See* Schwartz, *supra* note 251, at 301. There are three zones where such information is used: "zone one is direct patient care (doctors, clinics, nursing homes); zone two consists of supporting and administrative activities (service payers, third party administrators, quality of care reviewers); and zone three includes . . . 'secondary uses' [of medical data] (credential and evaluation decisions, public health reporting, social welfare programs, direct marketing)." *Id.* (citing Alan F. Westin, Interpretative Essay, *in* Harris-Equifax, Health Information Privacy Survey 7 (1993)).

371. *Id.*

372. Office of Technology Assessment, U.S. Congress, Protecting Privacy in Computerized Medical Information 13 (1993).

373. Sheri A. Alpert, *Smart Cards, Smarter Policy: Medical Records, Privacy and Health Care Reform*, 23 Hastings Center Rep. 13 (Nov.-Dec. 1993).

374. The Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment and Rehabilitation Act of 1970, 42 U.S.C. § 290ee-3 (1988); The Drug Abuse Office and Treatment Act of 1972, 42 U.S.C. § 290dd-2 (Supp. V 1993). Exceptions include the response to medical emergencies, court order, or in furtherance of scientific research. 42 U.S.C. § 290dd-2(b) (Supp. V 1993). These federal protections generally apply to government actions, but not to private actions. Schwartz, *supra* note 251, at 320. Private clinics for substance abuse that receive federal funds are required to adhere to federal standards for release of medical information, but privately funded facilities are not. *Id.*

375. Schwartz, *supra* note 251, at 318-19; *see infra* part II.G.2.

Congress requires the Department of Health and Human Services to provide data protection for Social Security records.[376] This measure, however, allows for disclosures "as otherwise provided by Federal law" and pursuant to regulations issued by the Secretary.[377]

The Americans with Disabilities Act ("ADA") prohibits employers from considering the disabilities of individuals in making employment decisions.[378] Yet individuals are likely unaware or unable to prove job discrimination based on health information.[379] Finally, the Age Discrimination in Employment Act ("ADEA")[380] prohibits the hiring or firing of employees based on age, but not for problems related to health.[381]

State privacy acts, which are modeled after the federal Privacy Act of 1974, provide some assurance that state-held medical records will not be disclosed to third parties without first obtaining the patient's consent.[382] These laws, however, do not succeed in overcoming the weaknesses in current federal data protection.[383]

The Uniform Health-Care Information Act,[384] which is subject to modification by state legislatures before passage, has been adopted by only a handful of states thus far.[385] Only two types of state health-

376. 42 U.S.C. § 1306(a) (1988). "Social security records often contain a variety of medical information . . . [which] is most typically collected in connection with claims for disability benefits." Schwartz, *supra* note 251, at 318 n.118.

377. 42 U.S.C. § 1306(a) (1988).

378. 42 U.S.C. § 12112 (Supp. V 1993).

379. *See* Robert L. Burgdorf Jr., *The Americans with Disabilities Act: Analysis and Implications of a Second-Generation Civil Rights Statute*, 26 Harv. C.R.-C.L. L. Rev. 413, 434-37 (1991); *see also* Dorothy Nelkin & M. Susan Lindee, The DNA Mystique: The Gene as a Cultural Icon 167 (1995) (stating that the ADA "does not preclude the use of 'sound actuarial data' as a basis on which to limit health care benefits"). Nelkin and Lindee are concerned that while laws such as the ADA may curb specific institutional abuses, it is harder to control popular and cultural attitudes that lead to informal discrimination based on knowledge of an individual's genetic information. *See id.*

For an interesting discussion of the Americans with Disabilities Act of 1990, see Rosemary E. Mahoney & Allan Gibofsky, *The Americans with Disabilities Act of 1990: Changes in Existing Protection and Impact on the Private Health Services Provider*, 13 J. Legal Med. 51 (1992).

380. 29 U.S.C. §§ 621-634 (1988).

381. *Id.*; Schwartz, *supra* note 251, at 319.

382. *See, e.g.*, Mass. Ann. Laws ch. 66A, § 2(c) (Law. Co-op. 1991) (requiring subject's authorization prior to release of information or authorized by statute in compliance with this chapter); Minn. Stat. Ann. § 13.04 subd. 2 (West 1995) (same); Ohio Rev. Code Ann. § 1347.05(G) (Anderson 1994) (requiring "reasonable precautions to protect personal information . . . from unauthorized . . . disclosure"); Va. Code Ann. § 2.1-382 (Michie 1995) (requiring notice to the individual prior to disclosure of personal information).

383. *See* Schwartz, *supra* note 251, at 320-24 (discussing state statutes concerning data protection).

384. *Id.*

385. Schwartz, *supra* note 251, at 322; *see also* Mont. Code Ann. § 50-16-501 (1993) (adopting the Act); Wash. Rev. Code Ann. § 70.02.005 to -.02.904 (West 1992 & Supp. 1995) (same).

record legislation are common to virtually every state.[386] Such state statutes require physicians, hospitals, and laboratories to file reports to state health care authorities concerning knife and gunshot wounds, sexually transmitted diseases, HIV infection, and communicable diseases, such as tuberculosis.[387] Second, most states recognize some type of provider patient-privilege.[388] In judicial proceedings, such a privilege permits the patient to restrict the physician (and sometimes other health professionals) from disclosing health information received by the patient in confidence.[389]

F. *Multimedia Transactions*[390]

Congress has passed several laws that address multimedia transactions and their inherent threats to privacy. This subsection discusses several of those laws.

1. Cable Television

Cable television systems can threaten consumer privacy because they have the capacity to collect and store information about "the behavior, information needs, and entertainment preferences of individuals."[391] In response to this threat, Congress passed the Cable Communications Policy Act of 1984 (the "1984 Cable Act"),[392] which imposes restrictions on the collection, use, and dissemination of subscriber information by cable systems operators, such as viewing habits of cable subscribers. This law requires cable operators to inform their subscribers annually of the nature of personally identifiable information collected about their subscribers, the cable company's disclosure practices, and their subscribers' rights to inspect and correct errors in such data.[393] The 1984 Cable Act permits operators to sell their mailing lists to third parties only if they have given their subscribers an

386. Unif. Health-Care Info. Act, 9 U.L.A. 475, 476 (1988) (prefatory note) [hereinafter Prefatory Note].

387. *Id.*; *see, e.g.*, Ark. Code Ann. § 12-12-602 (Michie 1987) (requiring the reporting of knife and gunshot wounds); Cal. Health & Safety Code § 199.21 (West Supp. 1995) (discussing HIV reporting requirements).

388. *Id.*

389. Prefatory Note, *supra* note 386, at 476. South Carolina, Texas, and Vermont do not have health care provider-patient statutes and are exceptions to this rule. *Id.* Most state statutes expressly allow the patient to waive this privilege. *Id.* Physicians can be compelled to give information in court-ordered examinations in cases of child abuse, involuntary hospitalization, and when a patient relies upon his medical condition as a defense. *Id.*

390. The NTIA Notice of Inquiry requested comments on multimedia transactions for March 1994. At the present time, we do not have copies of any comments.

391. Nimmer, *supra* note 223, ¶ 16.21.

392. 47 U.S.C. § 551 (1988 & Supp. V 1993).

393. *Id.*

opportunity to limit such disclosure, and such information does not reveal the viewing habits or other transactions of the subscriber.[394]

The Cable Television Consumer Protection and Competition Act of 1992 (the "1992 Cable Act")[395] extends the protections of the 1984 Cable Act to new wire and radio services that may be provided over cable facilities. In addition, the 1992 Cable Act requires cable operators to "take such actions as are necessary to prevent unauthorized access to such information by a person other than the subscriber or cable operator."[396]

2. Video

In 1988, Congress passed the Video Privacy Protection Act (the "1988 Video Act")[397] to protect the privacy of video cassette rentals and sales. For example, this law prohibits the disclosure of information that individuals have rented specific videos.[398] The 1988 Video Act also bars video cable service providers from disclosing to anyone the titles of video cassettes rented or purchased by a particular individual without that individual's consent. The 1988 Video Act, however, allows service providers to release customer mailing lists and subject matter (but not specific titles) of customer selections as long as the customer has been given the opportunity to object.[399]

3. Electronic Communications

Congress passed the Electronic Communications Privacy Act ("ECPA")[400] in 1986, amending the federal Wiretap Law[401] to include electronic communications. Prior to this amendment, the wiretap law covered only oral and wire (telephone) communications. The ECPA prohibits the unauthorized eavesdropping and interception of the content of e-mail, radio communications, data transmission, and telephone calls. The ECPA's concern is only with data in transit, rather

394. *Id.*

395. Pub. L. No. 102-385 § 20, 106 Stat. 1460, 1497 (1992) (codified in scattered sections of the Communications Act of 1934, 47 U.S.C. §§ 151-613).

396. *Id.* at 106 Stat. 1498.

397. 18 U.S.C. §§ 2710-2711 (1994).

398. The impetus behind this legislation was the public disclosure of Judge Robert Bork's video rental history when he was under consideration for the Supreme Court. Reidenberg, *supra* note 225, at 218.

399. 18 U.S.C. §§ 2710-2711 (1994).

400. Pub. L. No. 99-508, 100 Stat. 1848 (codified at 18 U.S.C. §§ 2510-2522, 2701-2711 (1994)). This law reversed the holding in Smith v. Maryland, 442 U.S. 735 (1979), in which the Supreme Court held that pen registers, a device in a telephone line to record the numbers called from that line, are not private. *Id.* at 741-42. The Court reasoned that callers could have no reasonable expectation of privacy regarding the numbers they called, given the knowledge that the numbers are communicated to the telephone company. *Id.* at 742.

401. 18 U.S.C. §§ 2510-2522 (1994). Wiretapping is a form of electronic or mechanical eavesdropping on phone calls or other communications. Black's Law Dictionary 1601 (6th ed. 1990).

than information that is being stored[402] or has already reached its destination.[403]

The ECPA specifically addresses the issue of stored information in a separate section, which protects e-mail from (1) unauthorized access, alteration and disruption, and (2) unauthorized disclosure. The first provision proscribes hacking-type activity,[404] while the second protects the privacy of e-mail from unintended recipients without authorization. Communications that are "stored" are not subject to stringent warrant requirements.

There has been very little case law interpreting the application of the ECPA to e-mail. Recently, the Fifth Circuit in *Steve Jackson Games, Inc. v. United States Secret Service*,[405] held that the ECPA does not require a court order to seize in-transit e-mail, including electronically stored information, i.e., electronic communications in a "temporary, intermediate storage . . . incidental to the electronic transmission thereof."[406]

In essence, the court sided with the Secret Service, which argued that the crucial factor is whether the message is sitting still or moving through the wires when it is caught by the government. The former situation requires a warrant; the latter does not. Hence, the Fifth Circuit ruled that information that had been posted on a bulletin board, but not yet read by its recipients, was not improperly seized.[407]

The ECPA will soon be tested in a federal court in Illinois, in what may be the first case addressing the privacy of employee voice mail in the workplace. In January of 1995, Michael Huffcut, a manager of a McDonald's restaurant in Elmira, New York, filed a lawsuit alleging that his former co-manager recorded personal voice mail messages that Huffcut had left for his lover (also a McDonald's employee) and played them for his wife.[408] Huffcut and his wife sued the restaurant

402. 18 U.S.C. § 2510(17) (1994). This section of the ECPA defines "electronic storage" as: "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and . . . any storage of such communication by an electronic communication service for purposes of backup protection of such communication." *Id.*

403. For the purposes of the ECPA, interception includes the acquisition of oral, wire, or electronic communications through an electronic, mechanical, or other device. Nimmer, *supra* note 223, ¶ 12.19[2]. Unauthorized interception of oral, wire, or electronic communications can result in both civil and criminal sanctions. 18 U.S.C. § 2701(b) (1994).

404. Computer hacking, whereby computer users break into private computer systems, is a felony offense. 18 U.S.C. § 1030 (1994).

405. 36 F.3d 457 (5th Cir. 1994).

406. *Id.* at 461 (quoting the ECPA, 18 U.S.C. § 2510(17), defining "electronic storage").

407. *Id.* at 463.

408. *Big Mac or Big Brother? Voicemail monitoring suit against McDonald's raises privacy issue*, INFORMATIONWEEK, May 1, 1995, at 49.

giant for $2 million in damages for emotional anguish, embarrassment, and loss of income.[409]

Huffcut claims that he had been assured that his voice mail access code number and messages were private. According to Professor Alan F. Westin of Columbia University, however, the ECPA "is framed in terms of live conversations and digitized data like E-mail. Voice mail seems to fall somewhere in between."[410] Professor Westin claims that companies may have good reason to be concerned about the "leaking of trade secrets, the quality of customer service, or even urgent messages from clients that could be sitting in the voice mailbox of an employee on sick leave."[411]

G. *Possible Legislation*

In recent years, Congress has considered various information privacy bills. At the close of the 103d Congress, a few bills were still pending. At the early stages of the 104th Congress, they had not yet been reintroduced. Below is a summary of a few of the bills.

1. Privacy in the Workplace[412]

The Privacy Workers and Consumers Act[413] would provide privacy protections in the workplace. This bill, which was introduced by Senator Paul Simon (D-Ill.) and Representative Pat Williams (D-Mont.) in 1994, would require employers to notify employees about how and when they are being monitored at work and grant them access to their files.

Privacy advocates believe such a law is long overdue. One organization, the 9-5 National Association of Working Women, reported that approximately fifty million people use computers and telephones at work on a daily basis.[414] Roughly half of these workers are monitored by their supervisors.[415] An informal survey of major Silicon Valley companies revealed that a majority retained the right to monitor employees' e-mail.[416] Some surveyed companies had no policy,

409. Rick Raber, *Companies Have Wide Latitude to Spy on Employees, as Two Lovers Find Out*, Buff. News, Apr. 24, 1995, at D11.

410. *Id.*

411. *Id.*

412. The ECPA, which updated wiretapping laws and outlawed e-mail interception on public electronic networks, was silent on the issue of workplace monitoring.

413. S. 984, 103d Cong., 1st Sess. (1993) (introduced by Sen. Paul Simon); H.R. 1900, 103d Cong., 1st Sess. (1993) (introduced by Rep. Pat Williams).

414. *Workers, Bosses Clash on Privacy*, Chi. Trib., Oct. 9, 1994, (Business), at 8.

415. *Id.*

416. Miranda Ewell, *E-Mail: Is the Boss Peeking?*, San Jose Mercury News, Apr. 18, 1994, at 1A. According to a 1993 survey for *Macworld*, 15% of the nation's companies monitor employees' performance by listening to voice mail. *Why Tap Voice Mail?*, USA Today, Mar. 3, 1995, at 8A. In the same survey, other forms of workplace monitoring are more prevalent, such as e-mail (42%) and reading computer files (74%). *Id.*

but no company said that it would not review their employees' e-mail.[417] Company executives often argue that, since they own the equipment, they should be able to monitor how it is being used.

2. Privacy of Medical Records

At the federal level, current laws governing medical data apply to information that is collected and managed by government agencies, not private businesses.[418] In 1994, Representative Gary Condit (D-Cal.) sponsored the Fair Health Information Practices Act,[419] which would ensure confidentiality of computerized medical records.[420] More than eighty percent of medical records, however, are on paper.[421] The bill would apply to everyone in the industry, including health care providers, researchers, public health officials, and others who require access to health data.[422] The current law only protects medical data in the hands of a physician, and may not protect information once it is transferred to an insurance company. The Condit bill would close this major gap in the law. The measure would also establish a uniform federal privacy standard and impose civil and criminal penalties upon those who improperly use patient data.[423]

Most recently, hearings have been conducted in the Senate on a bill known as the Medical Records Confidentiality Act of 1995.[424] The purpose of the bill is to provide increased control over one's own medical records with an emphasis on "confidentiality, access, and security."[425] Further, the bill would "provide the health care system

---

There have only been a handful of e-mail cases. *See supra* part II.F.3. Experts predict that the number will rise, however, because polls indicate that people are growing more and more concerned about their e-mail privacy. Last year, in one closely watched case, Hill v. NCAA, 865 P.2d 633 (Cal. 1994), the California Supreme Court ruled that state constitution provisions on privacy protect intrusions not only by government, but by business and other private parties. *Id.* at 644. Intrusions by a private party would not violate an individual right to privacy, however, if they were justified by "legitimate and important competing interests." *Id.* at 656. Thus, the California high court ruled that the National Collegiate Athletic Association had the right to monitor drug testing of Stanford athletes by observing urination. *Id.* at 669. Privacy advocates fear that this case may have a negative impact on e-mail litigation in the future.

417. Ewell, *supra* note 416, at 1A.

418. The Privacy Act of 1974 requires federal agencies to obtain written consent from people before releasing personal information and permits people to inspect and amend their files. 5 U.S.C. § 552a(b), (d) (1994).

419. H.R. 4077, 103d Cong., 2d Sess. (1994). This bill was reintroduced in the 104th Congress. *See* 141 Cong. Rec. E63 (Jan. 9, 1995).

420. *Id.*

421. 141 Cong. Rec. S15577 (Oct. 24, 1995) (statement of Sen. Bennett).

422. *Id.* (statement of Sen. Bennett).

423. *Id.* (statement of Sen. Bennett).

424. S. 1360, 104th Cong., 1st Sess (1995).

425. 141 Cong. Rec. S15577 (Oct. 24, 1995) (statement of Sen. Bennett).

with a Federal standard for handling identifiable health information."[426]

The bill would allow patients to restrict disclosure of medical data for other than treatment and billing purposes.[427] Moreover, health care providers would be required to maintain records of their disclosures.[428] Finally, the bill provides for both criminal and civil remedies.[429]

The bill has gained broad bipartisan support.[430] Some civil libertarians, however, have attacked the bill,[431] arguing that it would have the opposite effect of its stated purpose.[432] They believe that, as a result of the bill, large companies would have the ability to compile medical databases.[433] Despite the negative feelings that some people have toward the bill, Senator Bennett, the bill's cosponsor, stated that "[t]he prospects [for the bill's passage by this Congress] are extremely good."[434]

3. Consumer Credit Privacy

The Consumer Reporting Reform Act,[435] which was passed by the House in 1994, was awaiting Senate approval in the last Congress. The purpose of this measure, which was sponsored by Esteban Torres (D-Cal.), is to improve the accuracy of consumer reporting and to protect the privacy of consumers. Among other things, this bill would give consumers quicker and cheaper access to their credit files, and allow them the opportunity to opt out of having their name and personal data used for marketing purposes. This law would amend the FCRA.

III. The Need for Security

With the growing dependence on computers, there has also been a growing need for security measures through encryption. Personal and sensitive information online, including tax returns, medical records, welfare information, government bids, corporate trade secrets, credit card and bank data, and intimate conversations over wireless tele-

426. *Id.* (statement of Sen. Bennett).
427. *Id.* The bill would also permit patients to inspect and correct inaccuracies in their medical records, like they may do with their credit records. Gina Kolata, *When Patients' Records Are Commodities for Sale*, N.Y. Times, Nov. 15, 1995, at C14.
428. *Id.*
429. *Id.* at S15578-79.
430. Kolata, *supra* note 427, at A1.
431. *Id.*; Beverly Woodward, *Patients' Privacy at Risk*, N.Y. Times, Nov. 15, 1995, at A23.
432. *See* Kolata, *supra* note 427, at A1; *A Good Start Toward Medical Privacy*, N.Y. Times, Nov. 20, 1995, at A14.
433. *Id.*
434. *Id.*
435. H.R. 1015, 103d Cong., 2d Sess. (1994); S. 783, 103d Cong., 2d Sess. (1994).

phones, such as those that embarrassed the Prince of Wales,[436] can be intercepted. Even the National Football League is trying encrypted radio messages for last minute communications between coaches and players.[437] Encryption, however, has one major drawback—it protects law-abiding citizens, criminals, and spies alike. Thus, it has become increasingly urgent to find the proper balance between national security and individual privacy.

Cryptography—the technique of scrambling a message so that it can only be deciphered by the intended recipient, who knows the code—has been in existence for millennia. Julius Caesar is reported to have communicated in a secret code, replacing each letter by the third later letter in the Latin alphabet.[438] Until recently, cryptography has remained largely the domain of the military and diplomatic corps. In the computer age, however, cryptography has become essential in safeguarding the privacy of individual and corporate users of the information superhighway.

The Clipper Chip ("Clipper"), officially known as the "Key Escrow Encryption Program," is an encryption technology developed jointly by the National Institute of Standards and Technology ("NIST") and the National Security Agency ("NSA"), the federal organization charged with monitoring communications around the world. This tiny silicon chip was designed to enable the government to intercept coded telephone and computer communications. Clipper's cryptosystem is based on a highly classified mathematical algorithm, Skipjack, which scrambles data and voice transmission.

Each individual chip has a unique serial number and a "backdoor" that can only be opened by two electronic "keys," which themselves are algorithms. To prevent the government from potential abuse, these "keys" must be placed "in escrow" in separate data bases at the Treasury and NIST, and made available to law enforcement investigators only by court order.[439] According to the FBI, the Clipper Chip is sixteen million times stronger than its predecessor, Data Encryption Standard ("DES").[440]

436. An intimate conversation allegedly between Prince Charles and Camilla Parker Bowles, which took place on a cellular telephone, was intercepted. A transcript of the six minute tape was published by an Australian magazine, a German tabloid, and excerpted in the British tabloids. William Tuohy, *'Camillagate' May Keep Charles Off Throne*, L.A. Times, Jan. 14, 1993, at A14.

437. Steven Levy, *Battle of the Clipper Chip*, N.Y. Times, June 12, 1994, § 6 (Magazine), at 44, 50.

438. *See* Mark I. Koffsky, Comment, *Choppy Waters in the Surveillance Data Stream: The Clipper Scheme and the Particularity Clause*, 9 High Tech. L.J. 131, 133 (1994); Levy, *supra* note 437, at 47.

439. This is similar to the process currently used to grant law enforcement agencies permission to tap ordinary analog phone calls.

440. Dan Lehrer, *Clipper Chips and Cypherpunks*, The Nation, Oct. 10, 1994, at 376, 378.

Last May, the government adopted the Digital Signature Standard ("DSS"), an authentication code technology developed by NIST, which allows users to sign documents electronically and verify that they have not been altered. A more advanced version, Capstone, which incorporates DSS, can handle not only telephone communications, but also computer data transfers and data technology. In April 1993, President Clinton asked NIST to consider the Clipper Chip as a government standard, hoping that the key escrow system would balance two seemingly irreconcilable interests—privacy and security. During the period for public comment, the Administration received 331 letters and reports: 329 opposed (several from industry groups with many members) and only two in favor.[441]

One opponent, the ACLU, expressed its objections to policy initiatives that increase the government's ability to monitor activities of individuals and erode the protections guaranteed by the First, Fourth, and Fifth Amendments.[442] For example, the key escrow system would enable the government "to seize an encrypted communication and to search and seize the key to such communication" prior to establishing probable cause.[443] Moreover, the ACLU questioned the legality of a policy that regulates speech encoded in the form of a computer disk in the same fashion as weapons hardware.[444] The current export controls policy categorizes many encryption products as "munitions-related," thereby requiring a special export license.[445] In other words, one may export a book, but not a computer disk containing the same information, in an encrypted form.[446]

The White House formally adopted Clipper on February 4, 1994, amidst a swirl of public debate. Within a month, an anti-Clipper petition, circulated on the Internet by the Computer Professionals for So-

441. John Schwartz & John Mintz, *Clinton Plan for Wiretaps Taps Fears*, Wash. Post, Apr. 4, 1994, (Financial), at 17, 22.

442. Letter from Kate Martin, Center for National Security Studies, & Janlori Goldman, ACLU, to Computer Systems Security and Privacy Advisory Board 1 (May 28, 1993) [hereinafter ACLU Letter].

443. *Id.* at 4.

444. *Id.*

445. *See, e.g.*, Lance J. Hoffman et al., Institute for Computer and Telecommunications Systems Policy, Cryptography: Trends in Technology and Policy 9 (1994).

446. This oddity in the law was recently tested by Matthew Blaze, a researcher at AT&T who discovered a basic flaw in Clipper technology. *See infra* text accompanying note 464. Blaze applied for and received a temporary export license to bring a portable telephone encryption product with him on a business trip to Europe. Peter H. Lewis, *Between a Hacker and a Hard Place*, N.Y. Times, Apr. 10, 1995, at D1. Despite his having a license to export the device, Federal Customs agents at Kennedy International Airport in New York detained him for more than an hour while they puzzled over the "munitions" device, which they assumed to be a fancy weapon, in his carry-on bag. *Id.* "[I]t just isn't possible for an individual traveler to follow all the rules," concluded Blaze after the experience. *Id.* at D6. His days exporting arms were over, he added, at least until the laws are changed. "[N]ext time, I'm just not going to take it with me." *Id.*

cial Responsibility ("CPSR"), had collected 47,000 electronic signatures. Illinois Congressman John Anderson announced that he would serve on the advisory board of the Electronic Privacy Information Center ("EPIC"), a Washington-based group formed to pressure President Clinton to drop the Clipper proposal.

Senator Patrick J. Leahy, a Vermont Democrat who participated in a subcommittee debating the issue, expressed serious doubts "whether law-abiding users will want the government to hold the key to eavesdropping before any wiretap order is issued."[447] Concerned about America losing its competitive edge in the high-tech arena, Senator Leahy warned that "[t]he information superhighway would become a dead end at our border."[448]

The Clipper debate, dubbed the "Bosnia of telecommunications,"[449] has only intensified in recent months. The Clipper Chip has a broad spectrum of opponents, including civil liberties advocates, computer industry executives, cypherpunks, and Christian fundamentalists.

The most pressing issue is the government's export restriction of encryptions, other than Clipper. Privacy advocates insist that Clipper would impede the development of secure communications and have no effect on criminals who are too smart to use a device that the government can tap. After all, asked Daniel J. Weitzner, Deputy Director of the Center for Democracy and Technology, "if someone is planning a serious criminal conspiracy . . . the likelihood that they are going to go down to Radio Shack and buy the modem or buy the telephone that has stamped on it 'approved by the NSA' is very slim."[450] In addition, John Perry Barlow, a co-founder of the EFF,[451] a civil liberties lobbying group concerned with data network issues, stated: "Trusting the government with your privacy is like having a peeping Tom install your window blinds."[452]

The global market for strong encryption products has been growing steadily, and is potentially worth millions, if not billions, of dollars. Computer and software companies, such as Apple, IBM, and Microsoft lose tens of millions of dollars each year in potential export sales to foreign competitors. William Whitehurst, IBM Director of Data Security Systems, admitted that "[t]here's some definite uneven-

447. Patrick Leahy, *The Clipper Chip Solution*, Roll Call, June 27, 1994, at 12.

448. *Id.*

449. Levy, *supra* note 437, at 51 (quoting White House technology official Michael R. Nelson).

450. Association of the Bar of the City of New York, Panel Discussion on the Clipper Chip 13 (Jan. 19, 1995) (statement of Daniel J. Weitzner, Deputy Director, Center for Democracy and Technology) (on file with the *Fordham Law Review*) [hereinafter Policy Debate Transcript].

451. *See supra* part I.B. (listing EFF's comments to the Information Infrastructure Task Force Privacy Working Group Principles).

452. Jeff Rose, *Right to E-mail Privacy Would Seem Self-evident*, San Diego Union Trib., Mar. 1, 1994, (Computerlink), at 3.

ness in the implementation of export controls."[453] He continued, stating that "users would like freedom of choice . . . to protect their very valuable information."[454]

While installation of Clipper Chip is a "voluntary" industry standard,[455] the government's enormous buying power would make it essentially a de facto industry standard.[456] To facilitate sales of Clipper abroad, the State Department relaxed its export controls over Clipper while continuing to restrict other encryption methods.[457] That makes it difficult for commercial encryption systems to compete. And while Clipper is voluntary now, there is concern that if this system were ever to become mandatory, it could function like Prohibition on alcohol in the 1920s, encouraging black market activities and contempt for the law.

On the other hand, Clipper's defenders, who are largely in the government, believe that Clipper is the best option available to defend the nation against crime, terrorism, and external threats. The NSA claims that it must be able to decrypt any communication in the world

---

453. Policy Debate Transcript, *supra* note 450, at 23.

454. *Id.*

455. "Government officials say that even though Clipper has been endorsed as a new standard, everyone, including Government agencies, may use other encryption systems [domestically] in place of or in addition to it." Peter H. Lewis, *Of Privacy and Security: The Clipper Chip Debate*, N.Y. Times, Apr. 24, 1994, at 5; *see also* Koffsky, *supra* note 438, at 133-36 (noting that the use of the Clipper Chip is non-optional and positing a late extension to mandatory use). There are governmental restrictions, however, on the exportation of competing strong encryption systems. Lewis, *supra*, at 5.

456. *See* ACLU Letter, *supra* note 442, at 2; Letter from Computer Professionals for Social Responsibility to President Clinton 1 (Jan. 24, 1994) (on file with the *Fordham Law Review*) [hereinafter CPSR Letter].

457. For example, a state-of-the-art program called PGP (which stands for Pretty Good Privacy) was designed by Philip Zimmermann, a 41-year-old software wizard/activist based in Colorado. William M. Bulkeley, *Popularity Overseas of Encryption Code Has the U.S. Worried*, Wall St. J., Apr. 28, 1994, at A3. Whether it is more powerful than Clipper is unknown, because the Skipjack algorithm behind Clipper is classified. PGP, however, can also be used on top of Clipper.

Several years ago, a friend of Zimmerman's published the program on the Internet. *Id.* It quickly spread to many users in the United States and Europe. *Id.* One electronic message to Zimmerman from Latvia read, "If dictatorship takes over Russia, . . . your PGP is widespread from Baltic to Far East now and will help democratic people if necessary. Thanks." *Id.* at A3 (quoting the electronic message).

So far, PGP is uncrackable. In 1993, U.S. Customs Service agents questioned Zimmerman about his program being exported abroad without an export license. *Id.* at 8. Last spring, Zimmerman learned that he was targeted for grand jury investigation. *Id.* at 3. This raises interesting legal issues. For example, is it a crime to disseminate information legally in the United States that falls under the "munitions" category, thus requiring an export license, but which is accessible to network users worldwide? Is the First Amendment freedom of speech threatened by prohibiting overseas dissemination of information stored on a software disk?

Unfortunately, there is also a dark side to PGP: In 1993, it blocked the Sacramento police from reading the computer diary of a convicted pedophile and linking him to a suspected child-pornography ring. *Id.* at A3; Lehrer, *supra* note 440, at 376.

in order to protect the personal safety and national security of its citizens. NSA official Michael R. Nelson explained, "We are trying to keep this technology out of the hands of Moammar Khaddafi or the Hezbolah terrorist gangs in Lebanon .... We don't want this everywhere. . . . [W]e can insure that overseas this technology does not appear in every telephone in Libya."[458]

The FBI argues that traditional wiretap techniques, which entail little more than splicing into a telephone line and listening, are insufficient to protect society from modern criminals, especially terrorists.[459] One high-level FBI official stated that the damage resulting from the World Trade Center bombing is estimated at approximately $5 billion.[460] The NSA's former General Counsel Stewart A. Baker, stated that the only proposed alternative to government control of encryption is to allow access to everyone, including criminals.[461] He suggests that the choice is simple: "Would you rather trust this to the marketplace . . . or are you prepared to trust the democratic institutions . . . that have worked for our country . . . over the years?"[462]

American consumers are wary of purchasing an encryption program set up by the government. Further, industry officials fear that the Clipper's electronic "backdoor," which is an entry for legal wiretapping, would enable the government or unscrupulous civilians to eavesdrop without procuring a court order to obtain the "keys" held in escrow.[463] Moreover, last spring, a computer scientist at AT&T Bell Laboratories discovered a basic flaw in the Clipper technology that permits computer-savvy lawbreakers to encode messages that the government cannot crack.[464]

Last July, the Clinton Administration retreated from its encryption policy when it stated that the policy would apply to telephone conversations, but not to computers or other electronic communications.[465] Vice President Al Gore announced this change in government policy in a letter addressed to former Representative Maria Cantwell (D-

458. Policy Debate Transcript, *supra* note 450, at 21 (comment of Michael R. Nelson, Special Assistant for Information Technology, White House Office of Science and Technology Policy).

459. Policy Debate Transcript, *supra* note 450, at 7 (comment by James Kallstrom, FBI Special Agent in Charge of Special Operations Division in the New York Office).

460. *Id.*

461. Policy Debate Transcript, *supra* note 450, at 12 (comment by Stewart A. Baker, partner at Steptoe & Johnson and former General Counsel of the NSA).

462. *Id.*

463. John Markoff, *Flaw Discovered in Federal Plan for Wiretapping*, N.Y. Times, June 2, 1994, at A1, D17.

464. *Id.* at A1.

465. *See* Elizabeth Corcoran & John Mintz, *Administration Steps Back on Computer Surveillance: 'Clipper Chip' Use to be Limited to Phones*, Wash. Post, July 21, 1994, at A1, A10; *Washington Drops Spy Chip Plan*, Fin. Times (London), July 22, 1994, at 3 (discussing a letter from Vice President Al Gore to Maria Cantwell).

Wash.),[466] a one-term Congresswoman and Clipper foe who had negotiated directly with Gore regarding the policy.[467] Gore said that the administration would study the economic effect of export controls on encryption.[468] Gore's letter outlined "a framework for future negotiations on . . . how both to secure data transmissions and guarantee government access to them."[469] The new encoding standard "would be voluntary and would be exportable."[470] Last August, a group of hardware manufacturers sent a letter to Gore urging administrative action to liberalize export controls on equipment containing encryption technology other than Clipper. The software industry quickly followed suit, sending a letter on the Business Software Alliance's letterhead signed by Bill Gates of Microsoft, Jim Manzi formerly of Lotus and IBM, and others.[471] The letter requested "immediate action to liberalize export controls" to permit the inclusion of DES-level encryption in generally available software programs "so that . . . [they could] at least maintain [their] international position."[472]

Some critics, such as former EFF Executive Director Jerry Berman, see this change in policy as a "big step, both for privacy and security."[473] Others believe the government is just buying time. One policy analyst from EPIC, David Banisar, said that nothing has changed. "Clipper is the tip of the iceberg. . . . It's part of a big push by law enforcement to have their fingers in a lot of pies."[474] Further, it is not clear that the Administration has really made any concessions—most computers and faxes travel over telephone lines and switches. Thus, the Clipper debate continues.

---

466. *Washington Drops Spy Chip Plan*, *supra* note 465, at 3. Cantwell's district is the home of the software giant Microsoft, which is vehemently opposed to the Clipper Chip. *Id.*

467. Corcoran & Mintz, *supra* note 465, at A1.

468. *Id.* at A10.

469. *Id.* at A1.

470. *Id.*

471. Ted Bunker, *Government Ban on Scramblers Leaves U.S. Firms Out in the Cold*, Investor's Bus. Daily, Aug. 16, 1995, at A3.

472. *Id.*

473. Corcoran & Mintz, *supra* note 465, at A1. Although the administration has tried to create a de facto market for Clipper by encouraging federal agencies and the private sector to use it, Berman stated that "the fact is, there is no market for it." *Gore Letter on Clipper Chip Prompts Debate Over Interpretation*, Common Carrier Wk., July 25, 1994, *available in* LEXIS, News Library, CURNWS File.

474. Michael L. Rozansky, *Taking a Byte Out of Crime; Clipper Chip Stirs Protest Over Eavesdropping*, Houston Chron., July 31, 1994, (Business), at 2. Banisar contends that the NSA has too much influence and financial control over NIST and urges Congressional oversight of NSA. David Banisar, *Roadblocks on the Information Superhighway*, 41 Fed. B. News & J. 495, 502 (1994). Marc Rotenberg, director of EPIC, said the letter was a good first step, but did not resolve the security issues of encrypted messages. John Markoff, *Gore Shifts Stance on Chip Code*, N.Y. Times, July 21, 1994, at D1, D7. He declared that "[w]e cannot accept the key-escrow requirement," and stated that the inherent risks to privacy are "enormous." *Id.*

CONCLUSION

The information superhighway has been aptly termed the "Wild West," because it is an uncharted, open territory. Many privacy concerns are new; others are the same, but the contexts in which the concerns arise are different. The collection, storage, and dissemination of data are easier and cheaper than ever before. There are tremendous advantages to having such a vast array of information available. Indeed, "it is a basic tenet of our political and economic systems that more knowledge makes for better decisionmaking."[475]

American society is "at least ambivalent about the weight to assign to interests in personal privacy when they compete with the value of truthfulness."[476] The benefits derived from the flow of information should be weighed against the loss of control over security and individual privacy. Surely one of the greatest challenges ahead will be finding the proper balance.

475. Rochelle Cooper Dreyfuss & David W. Leebron, *Foreword: Privacy and Information Technology*, 1986 Ann. Surv. Am. L. 495, 496.

476. Diane L. Zimmerman, *Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort*, 68 Cornell L. Rev. 291, 326 (1983).