ARGUS RULES: THE COMMERCIALIZATION OF PERSONAL INFORMATION

Craig D. Tindall[*]

[W]ho could deny that privacy is a jewel? It has always been the mark of privilege, the distinguishing feature of a truly urbane culture. Out of the cave, the tribal teepee, the pueblo, the community fortress, man emerged to build himself a house of his own with a shelter in it for himself and his diversions. Every age has seen it so.[1]

I. INTRODUCTION

Everyone desires some degree of personal privacy. That desire is a natural result of an individual's interaction with society.[2] After all, one person alone on a desert island has little need for privacy.[3] Yet, it has become increasingly difficult to maintain the shelter from society that personal privacy once offered. Since the 1970s, a modern day Argus[4]—the corporate database—watches over virtually all of our activity in the marketplace.[5]

---

[*]Deputy City Attorney, City of Glendale, Arizona. B.S., Arizona State University (1982); J.D., Southern Methodist University (1991). All opinions expressed herein are solely those of the author and are not intended to reflect the position of any public or private entity.

1. PHYLLIS MCGINLEY, *A Lost Privilege, in* THE PROVINCE OF THE HEART 53, 56 (1959).

2. *See also* Roscoe Pound, *Interests of Personality*, 28 HARV. L. REV. 343 (1915) (describing how the legal recognition of the interests of personality resulted from society's progress); *see generally* Steven Hetcher, *Changing the Social Meaning of Privacy in Cyberspace*, 15 HARV. J.L. & TECH. 149, 150 (2001) ("Information privacy is a social goal, not a technological one."). *Cf.* U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 763 (1989) ("In an organized society, there are few facts that are not at one time or another divulged to another."); U.S. Dep't of Def. v. Fed. Labor Relations Auth., 510 U.S. 487, 500 (1994) ("An individual's interest in controlling the dissemination of information regarding personal matters does not dissolve simply because that information may be available to the public in some form.").

3. *See* Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1115 (2002).

4. "Argus had a hundred eyes in his head, and never went to sleep with more than two at a time, so that he kept watch of Io constantly." THOMAS BULFINCH, *The Age of Fable, in* BULFINCH'S MYTHOLOGY 7, 29 (1934).

5. DANIEL J. SOLOVE & MARC ROTENBERG, INFORMATION PRIVACY LAW 1 (2003) [hereinafter SOLOVE, INFORMATION PRIVACY LAW]. *See, e.g.*, Daniel F. DeLong, *Online Companies Have Your Number – and Want to Keep It*, NEWSFACTOR NETWORK (May 9, 2001), *at* http://www.newsfactor.com/perl/story/9472.html. *See also* Lawrence Jenab, *Will the Cookie Crumble?:*

Americans treasure their privacy.[6] Nevertheless, corporations with vast databases collect, analyze, use, and trade personal information about almost every American consumer. Over the last few years, the collection and use of consumer information has exploded with the advent of the Internet and online commerce.[7] During that time, consumers have become increasingly aware and alarmed by how this collection and use of personal information has devalued their privacy.

II. THE COMMERCIALIZING OF PERSONAL INFORMATION

The collection and use of personal information, unless checked, will unquestionably continue at an ever-increasing rate. The transformation of personal information into usable knowledge now drives a significant part of our economy.[8] Database technology and information processing techniques, such as "data mining"[9] and "personalization,"[10] allow businesses to produce alarmingly detailed "profiles" of millions of

---

An Analysis of Internet Privacy Regulation Schemes Proposed in the 106th Congress, 49 KAN. L. REV. 641, 641 (2001) (stating that it is indisputable that the online collection and sale of personally identifiable data has raised significant privacy concerns); Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 815 (2000) ("In the absence of effective limits, legal or otherwise, on the collection and use of personal information on the Internet, a new structure of power over individuals is emerging."). In February 2000, Michigan Attorney General Jennifer M. Granholm estimated that DoubleClick has accumulated 100 million consumer profiles through online tracking. Stephen Caswell, *Michigan Prepares to Sue DoubleClick for Spying*, E-COMMERCE TIMES, Feb. 18, 2000, *at* http://www.ecommercetimes.com/perl/story/2542.html. While online businesses and the Internet have done much to bring the issue of personal privacy and technology to the forefront, consumer profiling is hardly a new concern. *See generally* Arthur O'Connor, *Personalization: Coming Full Circle, Part 1*, ECRM GUIDE, June 21, 2001, *available at* http://ecommerce.internet.com/news/insights/trends/article/0,,3551_778061,00.html. Consumer profiling is also not limited to businesses that one normally associates with high technology. Consider the privacy implications of the increasingly ubiquitous supermarket discount card. These cards can track every purchase the holder makes and, over time, reveal a significant amount about the cardholder's tastes, physical condition, and potential desires. *See* Justin Rickard, *Trading Privacy for Grocery Money*, Privacy Foundation, *available at* http://www.privacyfoundation.org/resources/grocery.asp (last visited Aug. 23, 2003).

6. WHITE HOUSE, A FRAMEWORK FOR GLOBAL ELECTRONIC COMMERCE 16 (1997).

7. *See* FEDERAL TRADE COMMISSION, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE 1 (2000), *available at* http://www.ftc.gov/reports/privacy2000/privacy2000.pdf.

8. *See* Jenab, *supra* note 5, at 650 ("Personal details are acquiring enormous financial value. They are the new currency of the digital economy." (quoting Edward C. Baig, et al., *Privacy: The Internet Wants Your Personal Info., What's in it for You?*, BUS. WK., Apr. 5, 1999, at 84)); Cheryl Rosen & Beth Bacheldor, *The Politics of Privacy Protection*, Information Week, July 17, 2000, *available at* http://www.informationweek.com/795/prprivacy.htm.

9. According to Kurt Thearling, Ph.D., Chief Scientist, Wheelhouse Corporation, "[d]ata mining . . . is the automated extraction of predictive information from large databases." See generally Dr. Thearling's web page, which provides an excellent tutorial on various aspects of data mining. Thearling, *at* http://www.thearling.com (last visited Aug. 22, 2003).

10. Personalization is the design of marketing strategies based on the complex analysis of detailed personal information. *See* NATIONAL ASSOCIATION OF ATTORNEYS GENERAL, NAAG PRIVACY SUBCOMMITTEE REPORT: PRIVACY PRINCIPLES AND BACKGROUND (2000) [hereinafter NAAG REPORT], *available at* http://www.naag.org/naag/resolutions/subreport.php (last visited Sept. 2, 2003).

consumers.[11] Using these techniques, companies have developed new marketing strategies to target potential customers.[12]

The use of personal information for marketing purposes is not new. In the 1920s, for example, General Motors targeted potential customers by identifying owners of two-year-old Ford automobiles.[13] Modern technology has, however, made the commercial collection and use of personal information much more effective.[14] As a result, strategies such as personalization based on profiling,[15] have become prevalent marketing tools.[16]

The difference between personalized marketing eighty years ago and today is a matter of the amount and extent of the information that is available about targeted consumers. Beginning in the 1970s, profile-based personalized marketing hit the mother lode when the United States government began selling census data on magnetic tapes. Direct marketing companies such as Donnelley Marketing, MetroMail (now Experian), and R. L. Polk & Co. soon began combining this data with information from telephone books and voter registrations to build huge databases that profiled millions of consumers.[17]

Experian, for example, maintains a database of credit information on approximately 205 million people and demographic information on approximately 215 million consumers in 110 million households across the United States.[18] Donnelley Marketing claims to have "wide-ranging, up-to-date" consumer information on 225 million individuals and 100

---

11. *See, e.g.*, FEDERAL TRADE COMMISSION, ONLINE PROFILING: A REPORT TO CONGRESS (July 1999) [hereinafter ONLINE PROFILING: PART 1], *available at* http://www.ftc.gov/os/2000/06/onlineprofilingreportjune2000.pdf. *See also* FEDERAL TRADE COMMISSION, ONLINE PROFILING: A REPORT TO CONGRESS, PART 2 - RECOMMENDATIONS (July 2000) [hereinafter ONLINE PROFILING: PART 2], *available at* http://www.ftc.gov/os/2000/07/onlineprofiling.pdf. Online profiling is only one method of collecting data, but it is the method that has produced significant results for companies in the last few years. *Id.*

12. SOLOVE, INFORMATION PRIVACY LAW, *supra* note 5, at 492.

13. Roland Marchand, *Consumer Research as Public Relations: General Motors in the 1930s*, *in* GETTING AND SPENDING: EUROPEAN AND AMERICAN CONSUMER SOCIETIES IN THE TWENTIETH CENTURY 85, 85 (1998).

14. SOLOVE, INFORMATION PRIVACY LAW, *supra* note 5, at 1.

15. Profiling is the assembly of information about an individual's personal characteristics from various sources. *See* PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW 311 (1996) [hereinafter SCHWARTZ & REIDENBERG].

16. *See* SOLOVE, INFORMATION PRIVACY LAW, *supra* note 5, at 1; Stephanie Losi, *Personalization vs. Privacy: Rewriting the Rules*, CRMDaily.com (Jan. 22, 2001), *at* http://www.crmdaily.com/perl/story/6876.html; John Moore, *A Private Function*, E-BUSINESS, ZDNet Australia (Nov. 6, 2000), at http://www.zdnet.com.au/newstech/security/story/0,2000048600,20106874,00.htm. *See also* NAAG REPORT, *supra* note 10. The NAAG devoted their summer meeting to issues surrounding consumer privacy. *Id.* Highlighting the importance of these issues, it was noted in the report that this was the first time that this organization had devoted an entire meeting to one topic. *Id.*

17. DICK SHAVER, THE NEXT STEP IN DATABASE MARKETING 32 (1996).

18. Experian, Experian Factsheet, *at* http://www.experian.com/corporate/factsheet.html (last visited Nov. 19, 2003).

million unique households.[19] As of a few years ago, Catalina Marketing advertised that it had accumulated information about the supermarket buying habits of thirty million households.[20] R. L. Polk & Co., a storehouse of information about automobile purchasers, boasts that it:

> maintains a wide range of demographic data on households and individuals in the United States. Information is available on household income, age and gender of adults and children in the household, interests and hobbies of adults in the household, housing type and value, and many other demographic characteristics. These demographic characteristics can be appended to your customer list and you can select households for targeting based on these characteristics.[21]

A little-known Arkansas corporation, Acxiom, has profiled almost every American and millions of foreign households.[22] TransUnion Corporation, one of the largest credit bureaus in the United States, is reported to have electronic dossiers on three out of every four Americans.[23] Another organization, the Medical Information Bureau (now MIB, Inc.), has profiles of medical information on approximately fifteen million individuals that it has collected from its association of 600 insurance companies.[24] A company called ChoicePoint claims to have fourteen *billion* records on individuals and businesses that it can turn to for things such as pre-employment screening of job candidates.[25]

These are only some of the companies that gather and sell the consumer information that they have accumulated. Information about consumers also makes its way into many other databases, such as those of corporations gathering detailed information about their customers for their own use. In reality, scores of databases hold oceans of detailed personal information about hundreds of millions of people.

III. TRADING PRIVACY FOR COMMERCIAL BENEFITS

The fact that millions of individuals have been profiled and cataloged is interesting, but does it justify concern? After all, the use of personal information about consumers results in significant benefits for

19. Donnelley Marketing, Donnelley Content, *at* http://www.donnelleymarketing.com/prodserv/DonnelleyContent.htm (last visited Nov. 19, 2003).

20. Robert O'Harrow, Jr., *Behind the Instant Coupons, a Data-Crunching Powerhouse*, WASH. POST, Dec. 31, 1998, at A20.

21. Polk.com, Products and Services, Demographics, *at* http://www.polk.com/products/demographics.asp (last visited Aug. 23, 2003).

22. Dan Gillmor, *Corporations Have Feds' Ears in Privacy Debate*, ComputerWorld, Mar. 26, 2001, at 30, *available at* http://www.computerworld.com/securitytopics/security/privacy/story/0,10801,58964,00.html (last visited Aug. 23, 2003).

23. William Safire, *The Privacy President?*, N.Y. TIMES, Apr. 19, 2001, at A25.

24. *See generally* MIB, Inc., *at* http://www.mib.com (last visited Sept. 2, 2003).

25. ChoicePoint Online, *at* http://www.choicepointonline.com (last visited Aug. 22, 2003).

everyone.[26] For example, businesses that know a lot about their customers can obviously improve their efficiencies in marketing, distribution, and product development. This knowledge inarguably leads to the delivery of less expensive and more useful products and services.[27] Consumers are, therefore, largely trading privacy for a more efficient marketplace.[28] Perhaps because of these benefits, the loss of some personal privacy appears quite benign.

Businesses, it is argued, do not gather personal information about consumers to do harm.[29] This argument has always been much more troubling when made in another context. Governments have long claimed a need for personal information in order to service and protect their constituents. The governments have been forced, however, to weigh the desire to serve and protect against citizens' concerns for potential government abuses of the gathered information.[30] Such concerns were historically limited to governments because they were the only entities with the resources necessary to gather, analyze, and potentially misuse large amounts of personal information. Consequently,

---

26. *See, e.g.*, David Pogue, *Why I (Gulp) Don't Mind Targeted Ads*, *at* http://www.davidpogue.com (Oct. 11, 2001) (on file with the University of Illinois Journal of Law, Technology & Policy).

27. *See* NAAG REPORT, *supra* note 10; Kent Walker, *Where Everybody Knows Your Name: A Pragmatic Look at the Costs of Privacy and the Benefits of Information Exchange*, 2000 STAN. TECH. L. REV. 2 (Dec. 2000), *at* http://stlr.stanford.edu/STLR/Articles/00_STLR_2/index.htm.

28. For example, it has been estimated that information sharing in the financial services industry saved the customers of ninety financial institutions $17 billion a year and cut the costs of approximately 320 million person hours per year, accounting for thirty percent of the industry's revenues. ERNST & YOUNG L.L.P., CUSTOMER BENEFITS FROM CURRENT INFORMATION SHARING BY FINANCIAL SERVICES COMPANIES (Dec. 2000) (prepared for The Financial Services Roundtable), *available at* http://www.ey.com/global/content.nsf/US/Tax_-_Quantitative_Economics_and_Statistics_-_Library. *See also* Jim Castelli, *How to Handle Personal Information*, AMERICAN DEMOGRAPHICS, Mar. 1996, at 50 (arguing that privacy has been sacrificed for convenience and corporate profits). *See generally* Fred H. Cate & Michael E. Staten, *Putting People First: Consumer Benefits of Information Sharing* (Dec. 2000), *at* http://www.privacyalliance.org/resources/consumerbenies.pdf; THE WHARTON SCH. OF THE UNIV. OF PA., PUB. POL'Y & MGMT., UP FOR SALE: HOW BEST TO PROTECT PRIVACY ON THE INTERNET (Apr. 2001), *at* http://webi.Wharton.upenn.edu/St/articles/protectprivacyoninternet.htm (quoting Wharton legal studies professor Daniel Hunter: "[T]he current e-commerce system offers consumers free access to services that would otherwise cost money, such as browsers and access to e-mail, in return for the 'cost' of allowing companies to track their interests and general demographics. That, to me, is e-commerce industry's strongest argument for being allowed access to data generated by web usage."); John M. Barron & Michael E. Staten, *The Value of Comprehensive Credit Reports: Lessons from the U.S. Experience* (2000), *at* http://www.privacyalliance.org/resources/staten.pdf; AMITAI ETZIONI, THE LIMITS OF PRIVACY (1999) [hereinafter ETZIONI, THE LIMITS OF PRIVACY]; Amitai Etzioni, *A Contemporary Conception of Privacy*, 6 TELECOMM. & SPACE J. 81 (1999), *available at* http://www.gwu.edu/~ccps/etzioni/A270.html; Amitai Etzioni, *Podium: Rational Privacy Doctrine*, NAT'L L.J., May 17, 1999, at A21; Shane Ham & Robert D. Atkinson, *Online Privacy and a Free Internet: Striking a Balance*, PROGRESSIVE POLICY INST. (Apr. 2001), *at* http://www.ndol.org/documents/E-Privacy2.pdf; Rickard, *supra* note 5.

29. *E.g.*, Clyde Wayne Crews, Jr., *Policymakers Should "Opt Out" of Privacy Legislation*, CATO INST., *at* http://www.cato.org/dailys/03-13-01.html (Mar. 13, 2001); Solveig Singleton, *Privacy As Censorship: A Skeptical View of Proposals to Regulate Privacy in the Private Sector*, CATO INST., *at* http://www.cato.org/pubs/pas/pa-295.html (Jan. 22, 1998).

30. *See* Hetcher, *supra* note 2, at 161 n.42 (pointing out that privacy advocacy began in the 1960's in response to government data collection and the use of mainframe computers).

governments were the organizations against whom it was most difficult to insulate private lives.

Governmental organizations, of course, still gather massive amounts of personal information about their citizens.[31] Most citizens of free and democratic societies are cognizant of the potentially malevolent effects of this activity and maintain constant vigilance against potential government intrusions.[32] Fiction writers have fueled such vigilance with images of what it would be like without control over our private lives.[33] George Orwell, for example, vividly described what could result from the loss of control over personal privacy in his novel *Nineteen Eighty-Four*[34] and created the metaphor "Big Brother," which now universally stands for the government's potential ability to integrate information and technology into a vehicle for personal control.[35]

Although literary satire generally has focused on governments' intrusion into an individual's privacy, the fact is that businesses now easily rival governments' capacities to collect, analyze, and use detailed, personal data.[36] Consequently, limiting vigilance to government

31. SOLOVE, INFORMATION PRIVACY LAW, *supra* note 5, at 1. Governments still present significant privacy concerns. *See generally* Lucas Mast, *The Feds and Your Privacy*, CATO INST., *at* http://www.cato.org/dailys/09-27-00.html (Sept. 27, 2000) (discussing the Government Accounting Office's audit of government databases, the extent of private information held in these databases, and the poor job the government does to protect that information); DEPARTMENT OF HEALTH, EDUCATION AND WELFARE, RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS (1973), *available at* http://aspe.hhs.gov/datacncl/1973privacy/tocprefacemembers.htm (last visited Aug. 23, 2003) [hereinafter HEW Report].

32. In the United States, citizens commonly look to constitutional rights. While there is no specific mention of privacy in the U.S. Constitution or the Bill of Rights, the Supreme Court has found that there is a right of privacy implied in the Constitution's Amendments. *See, e.g.*, Griswold v. Connecticut, 381 U.S. 479, 484 (1965) (First, Fifth and Ninth Amendments); Katz v. United States, 389 U.S. 347, 350-51 (1967) (Fourth Amendment). A recent Fourth Amendment case, *Kyllo v. United States,* 533 U.S. 27 (2001), presents an interesting perspective on privacy protection in the face of technology. The Court ruled that the police could not validly use thermal-imaging technology to scan the defendant's home in search of marijuana-growing equipment. Several state constitutions also expressly provide for the right of privacy. *E.g.*, ARIZ. CONST. art. II, § 8; CAL. CONST. art. I, § 1; LA. CONST. art. I, § 5; MONT. CONST. art. II, § 10. Additionally, there are federal and state statutes to protect individual privacy against government intrusion. *See infra* note 59. For an in-depth study of the limitations on the protections against government intrusions, see generally SOLOVE, *Digital Dossiers*, *supra* note 3.

33. *E.g.,* GEORGE ORWELL, NINETEEN EIGHTY-FOUR (1949); ALDOUS HUXLEY, BRAVE NEW WORLD (1932); FRANZ KAFKA, THE TRIAL (1925). Kurt Vonnegut, whom *Time* magazine has described as "George Orwell, Dr. Caligari and Flash Gordon compounded into one writer," also offers a very interesting perspective on technology and societal control in *Player Piano* (1952).

34. ORWELL, *supra* note 33.

35. *Id. But cf.* RICHARD A. POSNER, ORWELL VERSUS HUXLEY: ECONOMICS, TECHNOLOGY, PRIVACY, AND SATIRE (The Univ. of Chicago L. Sch., John M. Olin L. & Econ. Working Paper No. 89, 2d series, 1999) (Judge Posner points out that Orwell's novel was less about the loss of privacy due to technology, which is what the metaphor "Big Brother" has come to stand for, than a pure satire of totalitarianism). For another interesting perspective on the literary metaphors of privacy, see generally Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393 (2001) [hereinafter Solove, *Privacy and Power*] (arguing that Orwell's novel does not well serve the current privacy debate and instead argues that Kafka's novel *The Trial* provides a better metaphor).

36. NAAG REPORT, *supra* note 10. *See also* ONLINE PROFILING: PART 1, *supra* note 11; ONLINE PROFILING: PART 2, *supra* note 11; Schwartz, *supra* note 5, at 852 (promoting government

intrusions is far too shortsighted.[37] As mentioned above, technology has made personal information a business commodity.[38] In that light, personal privacy, the gleam on the jewel of civilization and a prized American treasure, appears quite imperiled.

Despite this concern, little action has been taken against the loss of privacy that pervades today's marketplaces.[39] Consumers appear to be perfectly willing to offer businesses a startling amount of private information.[40] Few recognize the potential peril to their privacy, perhaps because of the pervasive assumption that the legal system protects consumers' personal privacy.[41]

That assumption is erroneous. In the United States, there is no right of privacy against private entities such as corporations. Short of some highly injurious or offensive use,[42] corporations can use personal information about customers in almost any manner they believe might be profitable.[43]

IV. THE LAW AND PRIVACY

The absence of a clearly recognized legal right of privacy in the common law stands apart from other legal systems throughout history.

---

action to protect privacy, Professor Schwartz states that the "private sector is as much the potential enemy of privacy as the State and, as a result, we must fear the government's inaction as much as its action.").

37. *See generally* ETZIONI, THE LIMITS OF PRIVACY, *supra* note 28.

38. For reports that document the beginning of concerns about computer databases and personal privacy, see HEW Report, *supra* note 31; NAT'L ACAD. OF SCI., PROJECT ON COMPUTER DATABANKS, DATABANKS IN A FREE SOCIETY (1972); CANADIAN DEP'T OF COMM. & CAN. DEP'T OF JUSTICE, PRIVACY AND COMPUTERS (1972); SWED. COMM. ON AUTOMATED PERS. SYS., DATA AND PRIVACY (1972). As mentioned above, businesses still have a learning curve when it comes to effectively using the personal information that they gather. *See, e.g.*, O'CONNOR, *supra* note 5 (describing some of the problems that business faces when attempting to implement an effective one-to-one marketing strategy using personal information about their customers).

39. *See, e.g.*, HARRIS INTERACTIVE, A SURVEY OF CONSUMER PRIVACY ATTITUDES AND BEHAVIORS (2001), *available at* https://www.bbbonline.org/UnderstandingPrivacy/library/harrissummary.pdf (last visited Aug. 23, 2003). Some studies find that this may be due more to a gap in knowledge about privacy issues. *See* Laura Rohde, *Surfers Want Privacy: Americans Want Net Privacy, but Don't Know How to Protect Themselves*, WEBBUSINESS MAG., Sept. 2000, (quoting a Pew Internet & American Life Project survey that found that "56% of those polled did not know that cookies are the primary online tracking tool, and only 10% had set their browsers to reject cookies as a way to protect their privacy"). Other authors suggest that consumer interest in privacy is merely superficial. Singleton, *supra* note 29 (citing STEVEN E. MILLER, CIVILIZING CYBERSPACE: POLICY, POWER AND THE INFORMATION SUPERHIGHWAY 265 (1996).

40. "[W]ithout knowing it you are providing large amounts of personal data to businesses that are free to sell this information, share it, or use it to make decisions that can affect your well-being. Furthermore, you are not being told that this information is being gathered, by whom or for what purpose." *Up for Sale, supra* note 28.

41. Pound, *supra* note 2.

42. *See infra* note 56 and accompanying text. *See generally* RESTATEMENT (SECOND) OF TORTS §§ 652B–652E (1977).

43. *See* Hetcher, *supra* note 2, at 161 (noting that privacy advocates could argue against government intrusion using the Fourth Amendment but have had no success protecting against increasing imposition on information privacy by private entities).

For example, while the Hippocratic Oath is a professional standard and not a law, it reflects the societal norm that existed at its genesis in the fifth century B.C. The oath requires physicians to keep private the personal information obtained about their patients.[44] The *Mishneh Torah* (1170-1180), a record of the oral laws of ancient Israel that was transcribed in approximately 200 A.D., also prescribed legal protection for privacy, declaring "the harm of being seen in private is a legal wrong."[45]

In 1948 the United Nations determined that privacy is a fundamental human right, stating, "[n]o one should be subjected to arbitrary interference with his privacy."[46] The Council of Europe, also viewing privacy as a human right, resolved in 1950 that "[e]veryone has the right to respect for his private and family life . . . ."[47] In 1995, the European Union perpetuated that resolution by issuing a directive intended to protect individual privacy against corporate intrusion.[48]

Although protected as a basic human right in some legal systems, American law developed little in the way of privacy protection from corporate entities. For many years, the need did not exist. Individuals could easily shelter their private information by simple, practical means. Technological advances changed that by making the shelter of privacy difficult, and in some cases impossible to maintain. Surprisingly, technology's erosion of privacy has been on-going for some time.

In 1890, technological changes prompted Louis Brandeis and Samuel Warren to write an article entitled *The Right of Privacy*.[49] At that time, developments in photography had made it possible to photograph a person without the individual having to sit perfectly still for several minutes, as was previously required by older equipment.[50] Spontaneous pictures became possible, and photographs taken without express consent from the subject became popular in newspapers. This created significant consternation within the genteel society of that era

---

44. See Nat'l Kidney & Transplant Div. of Urology, *The Hippocratic Oath*, *at* http://members.tripod.com/nktiuro/hippocra.htm (last updated Jan. 17, 1999) for a translation of both the original and modern version of the Oath. With respect to privacy, the original oath stated: "Whatever, in connection with my professional practice, or not in connection with it, I see or hear, in the life of men, which ought not to be spoken of abroad, I will not divulge, as reckoning that all such should be kept secret." *Id.* The modern version of the oath changes the commitment very little: "Whatever in connection with my professional practice or not in connection with it I may see or hear in the lives of my patients which ought not be spoken abroad, I will not divulge, reckoning that all such should be kept secret." *Id.*

45. MISHNEH TORAH, *Neighbors* 11, 14, THE CODE OF MAIMONIDES, BOOK XII: THE BOOK OF ACQUISITION, 165 (Julian Obermann ed., Isaac Klein, trans., Yale Univ. Press 1951).

46. G.A. Res. 217 A(III) art. 12, U.N. GAOR, 3d Sess., Supp. No. 13, at 71, U.N. Doc. A/810 (1948), *available at* http://www.un.org/Overview/rights.html (last visited Aug. 27, 2003).

47. Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 1, 1998, art. 8, ETS No. 005, Council of Europe, *at* http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm (last visited Oct. 24, 2003).

48. Council Directive 95/46/EC, 1995 O.J. (L 281) 31.

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

50. SOLOVE, INFORMATION PRIVACY LAW, *supra* note 5, at 47.

whose sense of decorum and propriety was violated by such "offensive" conduct.[51] A person, they argued, should have the right to choose to keep his or her likeness private.

Unfortunately, the law did not support that notion. Therefore, Brandeis and Warren sought to develop a legal framework that would protect personal privacy. They argued eloquently in favor of a distinct right to privacy, and they were highly influential.[52] They failed, however, to fuel the development of a comprehensive privacy right.[53]

Just as in Brandeis and Warren's day, technology is again applying substantial pressure to the boundaries of privacy in our legal system. Since the dawn of the twentieth century, there has been significant thought on the issue of personal privacy. In 1974, the Department of Health, Education, and Welfare developed what later became known as the Fair Information Practices Principles.[54] This work has been extremely important to the formation of modern legal thought about

---

51. Warren & Brandeis, *supra* note 49, at 195. Warren was Brandeis's former law partner and a noted lawyer in his own right. By this time, however, he had actually stopped practicing law and turned to running the family paper's empire. The story often told is that Mrs. Warren's anger over the publication of photographs taken at her daughter's wedding reception prompted Warren to convince Brandeis to write the article with him. That has been disputed. *See* James H. Barron, *Warren and Brandeis, The Right to Privacy,* 4 HARV. L. REV. 193 (1890): *Demystifying a Landmark Citation*, 13 SUFFOLK U. L. REV. 875 (1979) (pointing out that Warren's oldest daughter was only 10 years old in 1890).

52. SOLOVE, INFORMATION PRIVACY LAW, *supra* note 5, at 3; 62A AM. JUR. 2D *Privacy* § 2 (1990) (noting that the Brandeis and Warren article "synthesized at one stroke a whole new category of legal rights and initiated a new field of jurisprudence"). Harvard Law School Dean Roscoe Pound noted that this article "did nothing less than add a chapter to our law." Nicholas D. Bieter, *Minnesota's Right of Privacy Torts: Expanding Common Law Beyond Its Reasonable Constitutional Bounds in* Lake v. Wal-Mart Stores, Inc., 20 HAMLINE J. PUB. L. & POL'Y. 177, 181 (1998) (citations omitted). *See also* A.T. MASON, BRANDEIS: A FREE MAN'S LIFE 70 (1946); William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 383 (1960). The first recorded judicial recognition of a "right of privacy" in this country occurred shortly after the Brandeis article was published. MacKenzie v. Soden Mineral Co., 18 N.Y.S. 240, 249 (Sup. Ct. 1891). That case makes mention of a "reasonable right of privacy." *Id.* Soon thereafter, two more cases make mention of a right of privacy, although neither uphold that right under the circumstances presented in each case. Corliss v. E.W. Walker, 64 F. 280, 282 (1894); Schuyler v. Curtis, 42 N.E. 22, 27 (N.Y. 1895).

53. RICHARD F. HIXSON, PRIVACY IN A PUBLIC SOCIETY: HUMAN RIGHTS IN CONFLICT 49–51 (1987).

54. HEW Report, *supra* note 31. There were five core principles developed from the HEW Report. These are:

1. Notice/awareness: Consumers should be given notice of an entity's information practices before any personal information is collected from them.
2. Choice/consent: Consumers should be given an option as to how any personal information collected from them may be used, including secondary uses of the information.
3. Access/participation: Consumer should have access to the information and have a means of contesting the information accuracy or completeness.
4. Integrity/security: Entities collecting information should take reasonable steps to protect that information from loss, unauthorized access, destruction, use or disclosure.
5. Enforcement/redress: Consumers should have the ability to ensure compliance with the core information practice principles.

Id. See generally ONLINE PROFILING: PART 1, *supra* note 11; ONLINE PROFILING: PART 2, *supra* note 11; PRIVACY ONLINE: FAIR INFORMATION PRACTICES, *supra* note 7. The recognized need for statutory protection is not exactly new, *see e.g.*, AMERICAN ENTERPRISE INSTITUTE FOR PUBLIC POLICY RESEARCH, PRIVACY PROTECTION PROPOSALS (1979).

privacy. Although many countries have incorporated some form of the Fair Information Practices Principles into their privacy laws,[55] they remain absent in any comprehensive sense from legislation in this country.[56] While these principles are generally recognized as valuable,[57] our judiciary has completely ignored them.[58]

In an effort to change that fact, the last few years have seen a multitude of statutes proposed in Congress and in legislatures across the country.[59] The privacy legislation that has been enacted protects private information only in a piecemeal fashion, addressing specific areas that are commonly recognized as highly private and unquestionably due legal protection.[60]

---

55. DAVID FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES: THE FEDERAL REPUBLIC OF GERMANY, SWEDEN, FRANCE, CANADA, AND THE UNITED STATES (1989); *see also* Council Directive 95/46/EC, *supra* note 48.

56. *See* SOLOVE, INFORMATION PRIVACY LAW, *supra* note 5, at 565, 687 (noting that some piecemeal privacy legislation has incorporated Fair Information Practices, *e.g.*, Gramm-Leach-Bliley Act, 15 U.S.C. § 6801, *et. seq.*, but the principles have not been adopted in any comprehensive manner). *See generally* Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497 (1995).

57. *See, e.g.*, HEW Report, *supra* note 31; ONLINE PROFILING: PART 1, *supra* note 11; ONLINE PROFILING: PART 2, *supra* note 11; PRIVACY ONLINE: FAIR INFORMATION PRACTICES, *supra* note 7.

58. A Westlaw search of all cases for the term "FAIR INFORMATION PRACTICES PRINCIPLES" produced only one case, Hinderliter v. Humphries, 297 S.E.2d 684 (Va. 1982), which noted Virginia's Privacy Protection Act of 1976, VA. CODE ANN. §§ 2.1-377-386 (1976) (current version at VA. CODE ANN. §§ 2.2-3800(A)-3809 (2003)).

59. As of March 2003, the Electronic Privacy Information Center (EPIC) reported that there were 44 privacy-related bills introduced in the 108th Congress and 245 bills related to privacy introduced in the 107th Congress. Electronic Privacy Information Center, *at* http://www.epic.org (last visited Oct. 24, 2003). Additionally, over 300 privacy-related bills were introduced in the state legislatures during the beginning of 2001. Doug Brown, *Congress Readies for Privacy Fight*, INTERACTIVE WEEK, *available at* http://cma.zdnet.com/texis/techinfobase/techinfobase/+owo_qr+_sKs8K/zdisplay.html (Jan. 29, 2001). President George W. Bush is quoted as saying, "I believe that privacy is a fundamental right, and that every American should have absolute control over his or her personal information." Michael J. Miller, *Bush's Privacy Plan*, PC MAGAZINE, Jan. 22, 2001, available at http://www.pcmag.com/print_article/0,3048,a=4460,00.asp (last visited Oct. 24, 2003). Nevertheless, many privacy proponents were disappointed when the Bush White House announced that the President would not appoint a chief counselor for privacy, a position that had been created by the Clinton administration. Instead, responsibility for privacy was placed within the White House Office of Management and Budget. Patrick Thibodeau, *Bush Makes Key Privacy Decision: Administration Won't Appoint Privacy Czar*, COMPUTERWORLD, Apr. 16, 2001, available at http://www.computerworld.com/securitytopics/security/privacy/story/0,10801,59647,00.html (last visited Oct. 24, 2003).

60. *See, e.g.*, Cable Communications Policy Act of 1984, 47 U.S.C. § 551 (2000); Children's Online Privacy Protection Act of 1998, 15 U.S.C. § 6501 (2000); Children's Internet Protection Act of 2000, 20 U.S.C. § 7001 (2000); Communications Act of 1934, 47 U.S.C. § 222 (2000), *amended by* Telecommunications Act of 1996, 47 U.S.C. § 222 (2000); Comprehensive Crime Control Act of 1984, 18 U.S.C. § 3141 (2000); Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2000); Driver's Privacy Protection Act of 1994, 18 U.S.C. § 2721 (2000); Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510–2522, 2701–2711 (2000); Electronic Funds Transfer Act of 1978, 15 U.S.C. § 1693 (2000); Fair Credit Reporting Act of 1970, 15 U.S.C. § 1681 (2000); Fair Credit Billing Act, 15 U.S.C. § 1666 (2000); Fair Debt Collections Practices Act, 15 U.S.C. § 1692 (2000); Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232(g) (2000); Financial Services Modernization (Gramm-Leach-Bliley) Act of 1999, 15 U.S.C. § 6801 (2000); Freedom of Information Act, 5 U.S.C. § 552 (2000); Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 1320(d) (2000); Identity Theft and Assumption Deterrence Act of 1998, 18 U.S.C. § 1028 (2000); Privacy Act of 1974, 5 U.S.C. § 552(a) (2000); Privacy Protection Act, 42 U.S.C. § 2000(a) (2000); Telephone Consumer

Additionally, the common law recognizes some privacy torts. These are related to four interests: intrusion into a person's seclusion, disclosure of private information, misappropriation of one's likeness, and representation of a person in a "false light."[61] Privacy torts, however, seek to remedy only the more egregious acts that impose upon personal sanctity.[62]

Moreover, tort law, being compensatory in nature, necessarily operates most effectively after-the-fact. While tort law does have an inherent deterrent effect, it is of little measure with respect to privacy in the commercial context. For example, companies generally attempt to modify their behavior in order to avoid undue exposure to tort liability. Their efforts, however, are subject to economic weighing—if an activity presents a risk of loss that is less than the potential economic benefit derived from the activity, then, from an economic standpoint, engaging in the activity would be advantageous.[63] Consumer claims for privacy violations present a low economic risk to corporations who collect and use personal information. Therefore, the collection of personal information for marketing purposes rarely, if ever, creates the type of economic damage that would act as an effective deterrent against abuse.

Instead, the harm visited upon consumers by a loss of privacy is more emotional—a feeling of powerlessness and loss of personal security. Tort law provides no useful remedy and virtually no deterrent effect for these types of injuries.[64] Consequently, tort law cannot provide an effective method of protecting individual consumers from invasion by commercial entities.[65]

Lacking comprehensive statutory and tort protection, consumer privacy is exposed to violation and the law has failed to develop meaningful protection for more than a century. Undoubtedly, the reason lies with the recognition that the use of consumers' personal information provides more benefit than the need to protect consumer privacy. Technology, however, has now significantly increased the level of privacy's exposure to violation. Therefore, the balance of consumer privacy has shifted toward the need for increased protections.

Protection Act of 1991, 47 U.S.C. § 227 (2000); Telemarketing and Consumer Fraud and Abuse Prevention Act of 1991, 15 U.S.C. § 41 (2000); Right to Financial Privacy Act of 1978, 12 U.S.C. § 3401 (2000); Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (2000).

61. RESTATEMENT (SECOND) OF TORTS §§ 652B–652E (1977). These torts were developed from Dean Prosser's seminal article on privacy. *See* PROSSER, *supra* note 52.

62. RICHARD A. EPSTEIN, DECONSTRUCTING PRIVACY: AND PUTTING IT BACK TOGETHER AGAIN 6–10 (John M. Olin Law & Econ., Working Paper No. 75, 1999).

63. This statement is clearly an oversimplification although the point made is still valid. Factors beyond the strictly financial considerations, such as public relations, good will, customer relations, employee relations, etc., would normally be incorporated into a comprehensive risk/benefit analysis.

64. Jenab, *supra* note 5, at 656; Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381, 2388 (1996); Diane L. Zimmerman, *Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort*, 68 CORNELL L. REV. 291 (1983).

65. SOLOVE, *Privacy and Power*, *supra* note 35, at 1434. *See, e.g.*, Shibley v. Time, Inc., 341 N.E.2d 337 (Ohio Ct. App. 1975); Dwyer v. Am. Express Co., 652 N.E.2d 1351 (Ill. App. 1995).

V. BALANCING CONTROL OVER PERSONAL INFORMATION

Internet commerce and its ability to increase the capability of commercial entities to gather and make use of consumers' personal information has made the law's ineffectiveness in the area of privacy much more apparent. Consequently, technology has made consumers increasingly aware that the privacy of their personal information is at risk.[66] It has not, however, altered the basic need for privacy protection

66. SOLOVE, INFORMATION PRIVACY LAW, *supra* note 5, at 491; LOSI, *supra* note 16 (quoting Susannah Fox, director of research at the Pew Internet & American Life Project: "Basically, Americans want to rewrite the rules about how companies track their activities"). *Contra*, Paul A. Greenberg, *E-Shoppers Choose Personalization Over Privacy*, E-COMM. TIMES (Jan. 4, 2000), *at* http://www.ecommercetimes.com/perl/story/2131.html. There are data that suggest consumers have been aware of privacy intrusions for more than a decade. *See* SCHWARTZ & REIDENBERG, *supra* note 15, § 12-1, at 312 (noting that three of four Americans recognize they have lost control over their personal information, citing a poll by LOUIS HARRIS & ASSOC., EQUIFAX REPORT ON CONSUMER PRIVACY 4 (1992)). Businesses, in fact, are apparently beginning to recognize a desire on the part of consumers for privacy. *See, e.g.*, Jerri L. Ledford, *Akamai, Predictive Ally for Personalization with Privacy*, CRM Daily.com (Jan. 23, 2001), *at* http://www.ecommercetimes.com/perl/printer/6926/. Several recent surveys are beginning to reflect consumers' concerns. *See, e.g.*, Susannah Fox et. al., *Trust and Privacy Online: Why Americans Want to Rewrite the Rules*, The Internet Life Report, *at* http://www.pewinternet.org (Aug. 20, 2000) ("American Internet uses overwhelmingly want the presumption of privacy when they go online."); STATISTICAL RESEARCH, INC., HOW PEOPLE USE THE INTERNET 2001 (2001); UCLA CTR. FOR COMM. POLICY, THE UCLA INTERNET REPORT: SURVEYING THE DIGITAL FUTURE (Oct. 20, 2000), *at* http://ccp.ucla.edu/pages/internet-report.asp; NAT'L CONSUMERS LEAGUE, E-CONSUMER CONFIDENCE STUDY (2000), *at* https://www.nclnet.org/downloads/results.pdf (commission supported by Dell Computer Corp. and conducted by Harris Interactive). *But see* THE GALLUP ORGANIZATION, FEW USERS PAYING CLOSE ATTENTION TO INTERNET PRIVACY ISSUES (Aug. 27, 2000); Jim Harper & Solveig Singleton, *With a Grain of Salt: What Consumer Privacy Surveys Don't Tell Us*, COMPETITIVE ENTERPRISE INST. (June 2001), *at* http://www.cei.org/PDFs/with_a_grain_of_salt.pdf (providing a listing of surveys related to privacy that they reviewed from their article).

There are many groups that have taken up the cause of privacy advocacy. Other organizations have a clear mission to protect business' interests in the privacy debate. A few groups actually appear to seek a balance. A partial list of all these various organizations would include: American Civil Liberties Union (http://www.aclu.org); Americans for Computer Privacy (http://www.computerprivacy.com); Association for Competitive Technology (http://www.actonline.org); Call for Action, Inc. (http://www.callforaction.org); Center for Democracy and Technology (http://www.cdt.org); Center for Media Education (http://www.cme.org); Cookie Central (http://www.cookiecentral.com); Consumer's Union (http://www.consumersunion.org); Computer Professionals for Social Responsibility (http://www.cpsr.org); Direct Marketing Association (http://www.the-dma.org); Electronic Frontier Foundation (http://www.eff.org); Electronic Privacy Information Center (http://www.epic.org); Global Internet Liberty Campaign (http://www.gilc.org); Information Technology Association of America (http://www.itaa.org); Information Technology Industry Council (http://www.itic.org); International Security Trust & Privacy Alliance (http://www.istpa.org); Junkbusters (http://www.junkbusters.com); Network Advertising Initiative (http://www.networkadvertising.org); Online Privacy Alliance (http://www.privacyalliance.com); Personalization Consortium (http://www.personalization.org); Policy Counsel.com (http://www.policycounsel.com); Privacilla.org (http://www.privacilla.org); Privacy & American Business (http://www.pandab.org); Privacy Exchange.org (http://www.privacyexchange.org); Privacy Foundation (http://www.privacyfoundation.org); Privacy International (http://www.privacyinternational.org); PrivacyLaw.net (http://www.privacylaw.net); Privacy.org (http://www.privacy.org); Privacy Rights Clearinghouse (http://www.privacyrights.org); Progressive Policy Institute (http://www.ppionline.org); Public Interest Research Groups (http://www.pirg.org); BBB Online: Understanding Privacy (http://www.understandingprivacy.org).

Additionally, there are several government Web sites that address privacy issues: HHS Privacy Committee (http://aspe.hhs.gov/datacncl/privcmte.htm); Department of Health and Human

that has existed for some time; it has merely shifted the point at which consumers should be allowed to exercise control over the use of their personal information. The means by which personal information is collected—whether it is done online, via mail, or through direct interaction—does not matter. The shift caused by technology applies equally to any means of communication that implicates consumer privacy. In fact, the effectiveness of proposed privacy legislation has been measured by its equal application to both online and real-world transactions.[67]

Moreover, the principal discussions surrounding consumer privacy are equally concerned with online and traditional collection methods. These discussions focus on issues such as the right of consumers to trade personal information in exchange for some benefit,[68] the constitutional right to speak freely about others,[69] the property attributes of personal information,[70] and the inconvenience of absolute privacy.[71]

More importantly, regardless of how consumers' personal information is collected, one core issue remains paramount: control. The problem the commercial collection and use of personal information presents to privacy is that it deprives the consumer of any sort of meaningful control over his or her personal information.[72] Control is the essence of personal privacy. Because privacy is a necessary element of a high quality of life,[73] an individual's right to privacy cannot be denied.[74]

While some degree of control over personal privacy is necessary for an individual to experience a high quality of life, it is, of course, not the

---

Services (http://aspe.hhs.gov/admnsimp/); Department of Commerce (http://www.export.gov/safeharbor/ and http://www.ntia.doc.gov/reports/privacy/privacy_rpt.htm); Organization for Cooperation and Development (http://www.oecd.org/home/).

67. Jenab, *supra* note 5, at 665.

68. *See, e.g.*, Rickard, *supra* note 5.

69. *See generally* Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People From Speaking About You*, 52 STAN. L. REV. 1049 (2000); Singleton, *supra* note 29, at 7. *Contra* Paul M. Schwartz, *Free Speech vs. Information Privacy: Eugene Volokh's First Amendment Jurisprudence*, 52 STAN. L. REV. 1559 (2000).

70. *E.g.*, SINGLETON, *supra* note 29, at 13.

71. Scott McNealy, *The Case Against Absolute Privacy*, WASH. POST, May 29, 2001, at A15. Mr. McNealy, Chairman of Sun Microsystems, Inc., gained notoriety in the privacy arena when, at a press conference introducing Internet devices, he responded to a reporter's question about the impact of these devices, on personal privacy by quipping, "you have zero privacy anyway . . . get over it." For another analysis of the flawed nature of current privacy discussions, see Schwartz, *supra* note 5, at 815-16.

72. Solove, *Privacy and Power*, *supra* note 35, at 1422; U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 763 (1988) ("[B]oth the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person."). *But see* Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1097, 1109 (2002) (outlining the problems with equating the general concept of privacy with control); Schwartz, *supra* note 5, *at* 821-34 (describing the flaws in defining privacy as control over a property right).

73. FRED H. CATE, PRIVACY IN THE INFORMATION AGE 101 (1997).

74. *See* U.S. Dep't of Def. v. Fed. Labor Relations Auth., 510 U.S. 487, 501 (1994) (recognizing an individual interest in controlling the dissemination of personal information notwithstanding prior disclosure).

sole defining element of such a life.[75] "'Pure' privacy is no more desirable than no privacy."[76] Privacy must, therefore, be balanced with other important elements.

In seeking the proper balance between the individual's right to privacy and the benefits that flow from the use of personal information for commercial purposes, it is important to realize that social norms largely define the extent to which a consumer may legitimately exercise a right of privacy.[77] Individual privacy is based on the consumer's reasonable expectations of how personal information is handled.[78] The reasonableness of a consumer's expectations is, however, defined by the societal norms prevalent in the community.[79]

Interestingly, these norms are constantly being redefined.[80] Take, for example, the fact that intrusions into one's private affairs that once alarmed Brandeis' contemporaries seem quaint and wholly unrealistic today. Direct requests for personal information that a couple of decades ago would have been highly offensive are now regularly responded to without a second thought. Clearly, reasonable expectations of privacy are very different today than they were at the turn of the century.

Society may define the parameters of privacy, but it remains the individual consumer's responsibility to invoke the right of privacy. Each consumer's interest in privacy will vary. If, however, consumers' overall interest in privacy were to become too burdensome for society to maintain, reasonable expectations would have to shift to increase openness. Left to the market, this would most assuredly be a slow evolutionary process.

However, the evolution of society's privacy expectations no longer seems to work, if it ever did, on the same scale as bygone eras. Changes in technology over the last couple of decades have sped up the metamorphosis of privacy expectations. Revolutionary changes such as the war on terrorism will even more quickly alter our perception of what personal information may or may not be private. Our society is seeking the fulcrum upon which to balance personal privacy and the use of personal information in commerce. That balancing point will have to be established by a comprehensive legislative scheme.

VI. THE NEED FOR EFFECTIVE NOTICE

The political challenge of constructing such a statute has proven to be formidable. Nonetheless, the effort to create privacy legislation must

75. CATE, *supra* note 73, at 102.
76. *Id.* at 23.
77. *See generally* Hetcher, *supra* note 2.
78. *Id.*
79. *Id.*
80. *Id.*

continue. There are many issues that an effective statute must address;[81] for example, access to and the right to correct information that is collected, security of the information, remedies for breach, and governmental oversight.[82] Successfully addressing these issues will not, however, be the true measure of the effectiveness of new privacy legislation.

To be ultimately effective, the statute that protects consumers' right of privacy must do two things well. It must specifically define the types of information that will be considered private—in other words, establish the exception of privacy. Even more importantly, the statute must require an effective means of communication between the consumer and the companies seeking to use that consumer's personal information.

It is beyond the scope of this essay to suggest a comprehensive legislative scheme, nor does this essay seek to suggest how the privacy legislation should set social expectations. Instead, the remainder of this paper focuses on the communication between consumers and commercial entities that collect and use personal information, highlighting the proper starting point from which to develop legislation that effectively balances privacy in the commercial context.

In the discussion about the proper legislative scheme for consumer privacy, one of the most ardent debates is whether consumers should be allowed to "opt-in" or required to "opt-out" of the methods used to collect personal information for commercial purposes. Opt-in requires commercial users to secure permission from consumers before personal information is collected and used.[83] Opt-out allows for the collection and use of personal information unless consumers make the effort to disallow this activity.[84]

To a certain extent, the debate over opt-in or opt-out has been answered by practical experience.[85] One needs only to look to Europe's troubled experiment with an opt-in policy[86] to see the difficulty with, and probably the impossibility of, implementing an effective and comprehensive opt-in approach to consumer privacy.[87] Consequently, the most viable option is clearly to require that consumers desiring to protect their personal information conform to an opt-out legislative scheme.

---

81. Joel R. Reidenberg, *Restoring Americans' Privacy in Electronic Commerce*, 14 BERKELEY TECH. L.J. 771, 779-80 (1999).

82. *See generally* Jenab, *supra* note 5 (establishing a framework from which to analyze the privacy legislation that was proposed during the 106th Congress).

83. *See generally* Jeff Sovern, *Opting In, Opting Out, or No Options at All: The Fight for Control of Personal Information*, 74 WASH. L. REV. 1033 (1999).

84. *Id.*

85. *See, e.g.*, Jenab, *supra* note 5, at 667-68 (discussing the need for an opt-in approach and effectively summarizing in a succinct manner–albeit one contrary to the suggestions herein–the debate between opt-in and opt-out).

86. Council Directive 95/46/EC, *supra* note 48, at art. 7.

87. Carl Felsenfeld, *Unnecessary Privacy*, 25 SUFFOLK TRANSNAT'L L. REV. 365, 373-74 (2002).

Critics of the opt-out approach to privacy protection decry its enormous reliance on effective notice being given to consumers that their personal information is being collected and used.[88] They argue that consumers are currently too ill-informed about how their information is collected and used—the so-called "knowledge deficit"[89]—to make a well-reasoned decision to opt out. Because notices are ineffective, critics argue that the inability to overcome consumer ignorance makes opt-out an unworkable approach.[90]

Support for this argument is indeed found in the notices currently required by federal law. These notices are usually designed to provide a wealth of information. Take for example, the notice required by the Gramm-Leach-Bliley Act,[91] a portion of which is intended to protect personal financial information. Ostensibly, the notices required by this law were to inform consumers about how their financial information is collected, how it is to be used, and what legal protections might be available.[92] As a result of this law, every consumer in America has received dozens of privacy notices from financial institutions. It is probably fair to say that, contrary to the intent behind these notices, the general level of consumer knowledge about their financial privacy has changed very little, if at all.[93]

It is true that a majority of consumers may lack a comprehensive understanding of how information is collected and used, but consumers are not confused about the core issue of privacy. They understand very well how control over their privacy is lost when their personal information is being collected and used by another. The problem with the opt-out legislative approach is not so much consumer ignorance about the technical issues surrounding privacy, but the inability of consumers to clearly identify when it is time for them to take some action to protect their privacy. Notices that attempt to overcome the knowledge deficit with dense, legalistic, and overly complex documents will never effectively prompt consumers to take action.

---

88. *E.g.*, Jenab, *supra* note 5, at 667.

89. *See, e.g.*, Schwartz, *supra* note 5, at 821-29.

90. Jenab, *supra* note 5, at 667–68 ("Opponents [of industry self-regulation] cite the egregious failures of the self-regulatory regime as evidence that opt-out approaches would essentially lock in the existing low level of privacy, especially considering the widespread use of misleading or intentionally opaque statements of how personal information will be used . . . the user [is] confronted with ambiguous consent statements and gobbledygook lawyerese . . . ").

91. Financial Services Modernization (Gramm-Leach-Bliley) Act of 1999, § 6803, 15 U.S.C. § 6803 (1999).

92. *Id.*

93. European Law exemplifies the same problem. Articles 10 and 11 of the European Union Data Protection Directive require that "data subjects," i.e., consumers in the commercial context, be provided with notice that their personal information is being collected. That notice must contain certain information but its form is not mandated nor is the information that can be provided restricted. Lacking this direction, the notice provision of Europe's comprehensive privacy law is one of the reasons that the practical application of this law has not been as effective as many had anticipated. *See* Felsenfeld, *supra* note 83, at 373–74; FRED H. CATE, FINANCIAL SERVICES COORDINATING COUNCIL, OPT-IN EXPOSED 10–13 (2001), *available at* http://www.fsccnews.com/articles/cate_opt-in_FA.pdf.

Some consumers will care about their privacy and be prompted to protect personal information if given effective notice, and others will not. The vast majority of consumers will likely fall between these two extremes. Notices should seek to serve the spectrum of privacy concerns and not attempt to mold this spectrum into one homogenous mass of equally informed individuals. Instead, notices must be designed merely to trigger consumers' desire for control over their personal information.

Unfortunately, most proposed legislation reflects the prevailing thought that notices must be as comprehensive as possible. Such notices fail to serve consumers. Take, for example, the proposed Privacy Act of 2003 that was introduced before Congress as this paper was written.[94] That legislation, using the opt-out paradigm, is intended to provide a "comprehensive national system of privacy protection."[95] In summary, this bill prohibits a commercial entity from collecting personally identifiable information and disclosing that information to a third party for marketing purposes without notice and opportunity for the consumer to object. It also provides valuable protections for specific information such as social security numbers[96] and driver's license information,[97] and it attempts to clean up some of the privacy aspects of the Gramm-Leach-Bliley and the Health Insurance Portability and Accountability Acts.[98]

The notice provision of the Privacy Act of 2003 unfortunately follows the same errant path of previous privacy-related legislation. It does not attempt to define the form of the notice or restrict the information that might appear in the notice. As a result, notices under this proposed statute would be no different and no more meaningful than those currently in use. As a means of assisting consumers with their privacy decisions, these notices are destined to be useless and, as a result, the effectiveness of this proposed privacy legislation is doubtful even considering its many strong provisions.

Legislators must come to realize that most consumers have little time or inclination to read the long privacy notices. Therefore, to eliminate the ineffectiveness of the current concept of notice, simple

94. S. 745, 108th Cong. (2003) was introduced on March 31, 2003 by Sen. Diane Feinstein. 149 CONG. REC. S4559. As of April 2003, the bill was assigned to the Judiciary Committee. Analysis of the success of the bill is difficult at this point. It is likely that the bill will be strongly opposed by industry and, perhaps as a result, there has been no indication of widespread support from other legislators. This is not Sen. Feinstein's first attempt at privacy legislation. Previously, she introduced S. 600, The Personal Information Privacy Act of 1997, into the 105th Congress. *See* 143 CONG. REC. S3269 (1997). That bill, which had only one co-sponsor, failed to make it out of the Finance Committee. *See* S. 600, 105th Cong. (1997), *available at* http://thomas.loc.gov/bss/d105/d105laws.html.

95. 149 CONG. REC. S4559 (statement of Sen. Feinstein introducing The Privacy Act of 2003).

96. S. 745, *supra* note 90, tit. II – Social Security Number Misuse Prevention. This portion of the Bill was also introduced into the 108th Congress separately as a stand-alone bill, S. 228. *See* S. 745, 108th Cong. (2003), *available at* http://thomas.loc.gov/bss/d108/d108laws.html.

97. S. 745, *supra* note 90, tit. V – Driver's License Privacy.

98. S. 745, *supra* note 90, tit. III – Limitations on Sale and Sharing of Non-Public Personal Financial Information and tit. IV – Limitations on the Provision of Protected Health Information.

form notices are needed.[99] Limiting the amount of information in the notice will allow consumers to quickly read and understand what is being communicated. Prescribing the form of the notice will provide consumers with immediate access to that information. Most importantly, form notices will prevent companies from attempting to overwhelm consumers with enough information to foster inaction. It is consumer inaction that marks the ineffectiveness of privacy legislation.

The only purpose of such notices should be to motivate consumers to take the action they deem necessary to protect their private information. Attending only to that purpose, a simple yet effective notice could take following form:

> [Company or organization name] COLLECTS AND USES PERSONAL INFORMATION ABOUT ITS CUSTOMERS.
>
> THE TYPES OF PERSONAL INFORMATION WE COLLECT ABOUT YOU ARE: [list to follow].
>
> IF YOU PREFER THAT WE DO NOT COLLECT YOUR PERSONAL INFORMATION, PLEASE CALL US AT _____, E-MAIL US AT _____, OR RETURN THE ENCLOSED, SELF-ADDRESSED CARD AND WE WILL NOT USE ANY PERSONAL INFORMATION WE COLLECT EXCEPT TO COMPLETE THE CURRENT TRANSACTION.

If the company markets the personal information it collects about its customers to other entities, the following should be included:

> [Company or organization name] COLLECTS PERSONAL INFORMATION ABOUT ITS CONSUMERS AND PROVIDES THAT INFORMATION TO OTHER COMPANIES OR ORGANIZATIONS.
>
> THE TYPES OF PERSONAL INFORMATION WE PROVIDE TO OTHERS ARE: [list to follow].
>
> IF YOU PREFER THAT WE DO NOT PROVIDE YOUR PERSONAL INFORMATION TO OTHERS, PLEASE CALL US AT _____, E-MAIL US AT _____, OR RETURN THE ENCLOSED, SELF-ADDRESSED CARD AND WE WILL NOT DO SO.

99. Jenab, *supra* note 5, at 642-43 ("Notice requirements and consent mechanisms must be meaningful and should be calculated to provide actual notice and to facilitate privacy negotiations based on informed consent.").

This notice should be provided before the personal information is collected. This can be easily done in electronic transactions and could be attached, as a separate document, to written transactions. Even the small warranty cards upon which marketers have long relied for a wealth of personal information about consumers can easily carry this notice.

As mentioned above, notice alone is not a comprehensive legislative scheme. Additional details surrounding the process of protecting privacy must also be addressed. For example, the legislation should require that consumer responses be accepted in the same manner in which notice is provided. Furthermore, substantial penalties for non-compliance with either the notice requirement or a consumer's expressed desire to protect his or her privacy should also be implemented, including the right of private action for breach. Government oversight will be necessary and the Federal Trade Commission, for better or worse, seems to be the clear front-runner to take on this responsibility.[100]

With proper notice and the right to protect certain personal information, consumers can balance the benefits of allowing their personal information to be collected, used, and even disseminated. It is true that certain technical aspects of how information is collected and used will escape most people, but privacy in its most basic form is not complicated. The fact is that most rational people when told that their personal information will be collected, used, and perhaps sold for commercial purposes, will not grant permission for this to occur unless they care very little about their privacy.[101] This fact, of course, presents a significant problem for commercial entities.

Because most consumers will probably opt out and disallow the collection, use, and distribution of personal information, commercial users of private information will oppose simple form notices. The pretext of their objection will likely be that such notices fail to provide the consumer with enough information to make an informed decision. Of course, it is not an informed consumer about whom commercial entities are concerned. Informed consumers likely started protecting their privacy long ago. It is the barely-informed or uninformed consumers whom commercial users of consumers' personal information would prefer to continue to overwhelm with too much information in order to perpetuate these consumers' privacy paralysis. A consumer paralyzed by too much information will not opt out.

There is no reason to prohibit companies from exercising their considerable marketing power to convince consumers of the benefits of not opting-out. Marketers are very adept at convincing consumers to do

100. *See generally* Federal Trade Commission, *at* http://www.ftc.gov (last visited Oct. 22, 2003).

101. *Cf.* Schwartz, *supra* note 5, at 822-23 (discussing the notion of "bounded rationality," i.e., when consumers are left to fend for themselves, they will frequently accept whatever the industry offers).

all sorts of things; certainly, that ability can be used to communicate to consumers the benefits of allowing their personal information to be used. Such an arrangement may even spur the nascent information intermediary market as consumers decide how much personal privacy they are willing to exchange for the particular benefits made available by not opting-out. So long as marketing information is not provided in a manner that alters the form notice or impedes return communication from the consumer, the proper balance of consumer control can be achieved.

Notwithstanding the anticipated opposition to simple form notices, effective communication about privacy is the solid foundation upon which to build legislation that fairly balances the interests competing for consumers' personal information. Legislation that does not adequately prescribe the appropriate manner of communications between the consumers and commercial users of personal information will fail to provide appropriate privacy protection.

VII. EPILOGUE

The esteemed lawyer Louis Nizer once wrote:

> Once the right of privacy is recognized in its true light, its future development will be simple. It gives expression to an ideal which conceives of the individual as a unit not to be obliterated by society. Everyone has a right to live his own life in quiet and solitude.
>
> Carried to its ultimate extreme, this reasoning would lead to the destruction of social obligation. It is prevented from doing so by an opposing ideal which is as firmly established in the law—the realization that man is a social animal and in order to exist peaceably he must give up a portion of himself in return for the mutual advantages which flow from communal existence. There are times when the public interest demands disclosure of one's activities and achievements. So society, as an entity, also has rights—which are frequently paramount to the rights of the individual.
>
> The right of privacy is the child of these two opposite ideals. Like every new rule of law, it sprang from the spark struck off by clashing principles. With gradual adjustment of the weight given to these forces, a balance of values will be achieved and the right of privacy will reach its full stature as a mature expression of one phase of man's relations to his fellow-men.[102]

102. Louis Nizer, *The Right of Privacy: A Half Century's Developments*, 39 MICH. L. REV. 526, 560 (1941).

It is hard to describe the current state of affairs more accurately or eloquently; yet, this passage was written sixty years ago. The search for the proper balance between the rights of individuals and society continues, and probably always will, as technology continues to affect this balance and outpace the law. Nevertheless, technology seems to have brought us to a point where finding the proper balance is imperative. How and at what point that balance is achieved will likely define society in the future.[103]

It is inevitable that control over privacy be vested in individuals. In order for that to be accomplished, the most basic tenet of privacy control—notice to individuals that their personal information is being collected and used—must be adequately addressed. Clear, simple-form notices that are specifically defined by statute, coupled with a simple method for the consumer to affirmatively exercise action to deny use or dissemination of the information, are needed.

Obviously there are other important aspects of an effective privacy statute; but, incorporating simple-form notices into the statutory scheme will do much toward providing consumers with practical control over their private information.

As with any statute that seeks to change the status quo, passage of privacy legislation will take substantial political courage. Companies profit handsomely from the unrestricted collection and use of personal information, and they will use their considerable resources in an attempt to defeat any such privacy legislation. That effort, however, would be shortsighted. It is in the long-term interests of commercial users of personal information to support reasonable measures providing consumers with a sense of control. Otherwise, the perception that control has been lost will grow to a point where consumers will demand measures more likely to be inconsistent with maintaining the benefits that flow from a reasonable use of consumer information. The balance of an individual's rights and society's needs may then be inalterably skewed.

Americans treasure their privacy because it represents freedom. Privacy allows us the freedom to choose—to choose what we want to think, what we want to do, and what we want to acquire. More importantly, it allows us the choice to be left alone. To shelter ourselves from the gaze of society, to engage in our own diversions, or merely to be left alone are the freedoms that we have a natural right to enjoy—freedoms that the law must protect.

The unrestricted commercial use of personal information degrades these freedoms. That degradation is enhanced by current technology, and there can be no doubt that future technological advances will exacerbate the situation. Therefore, it is time for the law of privacy to

103. *See generally* Solove, *Privacy and Power*, *supra* note 35, at 1418-30.

catch up and provide the protection necessary to assure that individuals are able to maintain the jewel of civilization: personal privacy.