The Right to Privacy in Internet Commerce: A Call for New Federal Guidelines and the Creation of an Independent Privacy Commission

Christopher F. Carlton

Follow this and additional works at: https://scholarship.law.stjohns.edu/jcred

Recommended Citation
Available at: https://scholarship.law.stjohns.edu/jcred/vol16/iss2/7

This Article is brought to you for free and open access by the Journals at St. John's Law Scholarship Repository. It has been accepted for inclusion in Journal of Civil Rights and Economic Development by an authorized editor of St. John's Law Scholarship Repository. For more information, please contact lasalar@stjohns.edu.
THE RIGHT TO PRIVACY IN INTERNET COMMERCE:

A CALL FOR NEW FEDERAL GUIDELINES AND THE CREATION OF AN INDEPENDENT PRIVACY COMMISSION

CHRISTOPHER F. CARLTON*

“Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual .. the right to be let alone . . . [O]f the desirability—indeed of the necessity—of some such protection, there can, it is believed, be no doubt.”¹

I. INTRODUCTION

In an era that has been appropriately christened “The

* Mr. Carlton is with the law firm of Morris, Nichols, Arsh & Tunnell in Wilmington, Delaware. The views expressed in this Article are solely the views of the author. The author thanks Lisa Dukes for her assistance in preparing the Article for publication.

Information Age" the Internet is utilized in virtually every area of our society. The Internet is now used by approximately one-half of the adult population of the United States, making it "the fastest-growing medium in human history." For instance, it took television more than thirteen years and radio more than thirty-eight years to capture their respective comparable audience bases. But despite the explosive growth in the use of the Internet, confidence on the part of Internet users about their privacy is lacking which has stunted the Internet's development as a commercial medium.

Over the last twenty years, an overwhelming number of Americans have reported that they have lost the ability to control the collection and dissemination of their personal information and that the current laws are not enough to protect their right of privacy. Indeed, it is indisputable that our existing legal framework did not envision the pervasive role information technology would have on our society. Advancing technology coupled with a growing population thirsty for information has taken us to the point where the right of privacy has been sacrificed for the almighty dollar.

2 See Privacy in Electronic Communication, 1998: Testimony Before the Subcomm. on Courts and Intellectual Property, House Judiciary Comm., 105th Cong. 315 (March 26, 1998) (hereinafter "Hearings") (stating testimony of Fred H. Cate, Professor of Law, Ind., Univ. Sch. Of Law); see also Mark Ishman, Computer Crimes and the Respondent Superior Doctrine: Employees Beware, 6 B.U. J. SCI. & TECH. L. 6, 86 n.12 (June 1, 2000) (discussing explosive growth of Internet). But see Offline, On Purpose; In a Survey That Contradicts Other Findings, Millions of Americans Said They Don't Use the Internet and Don't Particularly Care to Start, STAR TRIBUNE (Minneapolis), Sept. 22, 2000, at 4A (reporting that majority of Americans who are not on Internet are not interested in gaining access).


4 See Keith H. Hammonds, ed., Business Week/Harris Poll: Online Insecurity, BUS. WK., Mar. 16, 1998, at 102 (reporting that consumers considered sacrifice in personal privacy to be "the top reason people are staying off the Web—above cost, ease of use and annoying marketing messages"). See generally Michael Grebb, Cable's Big Brother Problem; Internet and Interactive Privacy Becomes an Issue, CABLEVISION, Nov. 13, 2000, at 44 (discussing privacy issues brought forward by Internet); John Geralds, Lack of Privacy is Main Internet Worry, NETWORK NEWS, Nov. 1, 2000, at 7 (reporting that privacy is leading concern among Internet users).

5 See Karl D. Belgum, Who Leads at Half-time?: Three Conflicting Visions of Internet Privacy Policy, 6 RICH. J.L. & TECH. 1, 6 (1999) ("The Internet raises new threats to
The Internet poses a new set of challenges to privacy by its functions and use because of the relative ease with which information can be collected, sorted and disseminated. But the legal system has not sufficiently evolved and technological advances have made the legal protections developed over the last few centuries obsolete. The current policy of self-regulation whereby Internet users and operators are setting the rules and regulations has proven to be ineffective.

Nowhere on the Internet is this loss of personal privacy more apparent than in the area of Internet commerce. The Internet has the potential to become the supreme commercial marketplace—a virtual marketplace without walls where one may shop from the comfort of home. The potential profits to Internet merchants and the benefits to consumers from Internet commerce are limitless. But privacy fears have drastically slowed the public's acceptance of online commerce. According to a number of recent surveys, potential Internet consumers report
that privacy protection is their number one concern and that if privacy issues were effectively addressed, they would be more likely to make online purchases. It is therefore abundantly clear that effective protection of personal information is an essential precondition for social acceptance of the Internet as a commercial medium.

The purpose of this Article is to expose the ways computer technology has magnified the threat to informational privacy in online commercial transactions and to advocate for the implementation of comprehensive privacy legislation coupled with the creation of an independent privacy commission to oversee enforcement of the legislation. Implementation of those proposals would ease the trepidation held by prospective online consumers that is currently hindering the enormous growth potential of Internet commerce.

Part II of this Article provides an overview of the right of privacy in America and its application to electronic commerce. Part II also chronicles how the advent of electronic commerce has threatened our fundamental right of privacy. Part III examines the inadequate privacy safeguards currently in place. Part IV of this Article recommends that to ensure the vitality of electronic commerce, Congress should create a legal framework for protecting personal privacy in online commercial transactions and create an independent privacy commission to regulate that

9 See Seth Safier, Between Big Brother and the Bottom Line: Privacy In Cyberspace, 5 VA. J.L. & TECH. 6, 21 (Spring 2000) (citing survey in which 70% of consumers surveyed noted privacy concerns as their primary reason for not providing personal information to web sites); George B. Trubow, Regulating Transactions of the Internet, 24 OHIO N.U. L. REV. 831, 832 (1998) (stating that in Louis Harris-Alan Westin survey conducted in April 1998, eighty-seven percent of Internet user respondents said they were concerned about threats to personal privacy); see also Domingo R. Tan, Personal Privacy in the Information Age: Comparison of Internet Data Protection Regulations in the United States and the European Union, 21 LOY. L.A. INT'L & COMP. L. J. 661, 664 (1999) (citing Boston Consulting Group consumer survey in which more than 70% of consumers worry about making on-line purchases).

10 See Tan, supra note 9, at 665 (indicating that more internet users would go online if they felt their personal information would be better protected); see also Gerals, supra note 4, at 7 (reporting majority of individuals surveyed feel internet users risk their privacy every time they go online). See generally ARTHUR MILLER, THE ASSAULT ON PRIVACY 23 (1971) ("[I]t is essential to expose the ways computer technology is magnifying the threat to informational privacy - a threat that we have faced in some form ever since man began to take notes about himself and his neighbors.").

11 See infra notes 16-44 and accompanying text.
12 See infra notes 45-67 and accompanying text.
13 See infra notes 68-141 and accompanying text.
legislation and ensure that it remains viable in view of emerging technology.\textsuperscript{14} Finally, Part V of this Article concludes that these measures, or other comparable measures, are vital to the success of online commerce.\textsuperscript{15}

II. THE RIGHT OF PRIVACY AND ITS APPLICATION IN INTERNET COMMERCE

At the heart of the right to privacy in today's information age lies the political, social and economic values upon which early notions of personal privacy originated. Thus, to fully appreciate the right of privacy, an examination of privacy law must begin by defining the right of privacy and tracing its origins. At that point, current privacy protections can be assessed.

A. Defining The Right Of Privacy And Its Origins

Generations of lawyers, judges and legal scholars have long explored the many facets of privacy and from what the "right to privacy" originates.\textsuperscript{16} Commentators and the courts have consistently invoked such notions as natural rights,\textsuperscript{17} fundamental human values,\textsuperscript{18} or human dignity\textsuperscript{19} as the

\textsuperscript{14} See infra notes 142-55 and accompanying text.
\textsuperscript{15} See infra notes 156-61 and accompanying text.
\textsuperscript{16} See Millar v. Taylor, 98 Eng. Rep. 201, 242 (K.B. 1769) ("It is certain every man has a right to keep his own sentiments, if he pleases: he has certainly a right to judge whether he will make them public, or commit them only to the sight of his friends."); see also Warren & Brandeis, supra note 1, at 205-07 (advocating individual's right to privacy and remedies for its violation). See generally BARRINGTON MOORE, PRIVACY: STUDIES IN SOCIAL AND CULTURAL HISTORY (1984) (examining concept of privacy in various societies including 4th century BC Athens, ancient Hebrew society and ancient China).
\textsuperscript{18} See Moore v. City of E. Cleveland, 431 U.S. 494, 503-05 (1977) (noting that sanctity of family is protected because it is fundamental human value, part of nation's history and traditions); Roe v. Wade, 410 U.S. 113, 152-53 (1973) (holding that right of privacy granted by Constitution includes fundamental personal rights relating to marriage, procreation, contraception, family relationships, child rearing and education). See generally Edward J. Eberle, Human Dignity, Privacy, and Personality in German and American Constitutional Law, 1997 UTAH L. REV. 963 passim (discussing human dignity as foundation of privacy).
\textsuperscript{19} See Edward J. Bloustein, Group Privacy: The Right to Huddle, 8 RUTGERS-CAM. L.
foundations of privacy. But even though notions of rights of privacy have existed for hundreds of years, it was not until the last part of the Nineteenth Century that legal scholars first considered the notion of privacy as a legal right.

The modern right of privacy traces its origins to the seminal article on the subject co-authored by Samuel D. Warren and Louis D. Brandeis in 1890, in which they proclaimed that each person had the right “to be let alone.” Warren and Brandeis


20 See Griswold v. Connecticut, 381 U.S. 479, 484 (1965) (stating "various guarantees create zones of privacy"); Mapp v. Ohio, 367 U.S. 643, 656 (1961) (stating "right to privacy, no less important than any other right carefully and particularly reserved to the people"); see also Rob Reilly, Conceptual Foundations of Privacy: Looking Backward Before Stepping Forward, 6 RICH. J. L. & PUB. POLY 6, 11 (1999) (noting early nineteenth century Americans invented barbed wire and built fences along frontier, invented private Pullman compartment for railroad travel and have otherwise "continually sought to satisfy their desire to be let alone").

21 See Reilly, supra note 20, at 9 (explaining need for right of privacy at close of Nineteenth Century:

The emergence of a newly-industrialized society required a greater quantity and quality of information than did pre-industrial society. The U.S. labor force was migrating toward urban centers where industry was burgeoning. The aggregation of so many people into condensed areas greatly facilitated compiling information. This fostered a greater reliance on newly-developed machines, by which to boost the process of information gathering... This erosion [of an individual's ability to shield information about himself from the public] became more pronounced when, in 1876, the telephone was invented, followed closely by the invention of the radio. At that time, there was an increasing ability of information technology to pervasively intrude upon privacy.

see also FCC v. Pacifica Foundation, 438 U.S. 726, 750 (1978) (holding unique attributes of broadcasting can intrude on privacy of home without prior warning of content); Reno v. ACLU, 521 U.S. 844, 884-85 (1997) (striking down provisions of Communications Decency Act of 1996 criminalizing internet transmissions of obscene or indecent messages to any recipient under 18 for being unconstitutionally vague and overbroad).


authored their article to shed light on the fact that technology was in a perpetual state of evolution and that the American legal system must concomitantly evolve in order to protect an individual's right to privacy.\textsuperscript{24} From this influential article, the courts began to construct a number of privacy principles that generally became known as the "right of privacy."\textsuperscript{25} Developed incrementally on a case-by-case basis, those privacy principles provided individuals with privacy-related causes of action based upon the law of property, tort and contract.\textsuperscript{26}

Much later in judicial history,\textsuperscript{27} even though the term privacy is not defined or even mentioned in the U.S. Constitution, the United States Supreme Court deemed privacy rights so fundamental that it established a constitutional right of privacy through a line of decisions thereby enhancing existing common law principles.\textsuperscript{28}

*Privacy, 102 HARV. L. REV. 737, 752 (1989) (discussing Warren & Brandeis' interpretation of tort law right of privacy).*

\textsuperscript{24} See Warren & Brandeis, *supra* note 1, at 195-96 (stating mass media was "overstepping in every direction the obvious bounds of propriety and of decency"; such dangerous technology included "instantaneous photographs" and "newspaper enterprise"); see also David Grant, Comment, *Rights of Privacy-An Analytical Model for the Negative Rights of Attribution*, 1992 UTAH L. REV. 529, 531 (noting Warren's motivation for writing article, at least in part, was due to intrusiveness of reporters at his daughter's wedding); Alexander Rodriguez, Comment, *All Bark, No Byte: Employee E-Mail Privacy Rights in the Private Sector Workplace*, 47 EMORY L. J. 1439 (1998) (suggesting as technology moves forward and electronic communication is fully developed, lawmakers will be forced to ensure right to privacy).

\textsuperscript{25} See *Griswold*, 381 U.S. at 484 (recognizing constitutional right of privacy); EVAN HENDRICKS ET AL., YOUR RIGHT TO PRIVACY: A BASIC GUIDE TO LEGAL RIGHTS IN AN INFORMATION SOCIETY XIII (2d ed. 1990) (detailing origins of right to privacy); see also Matthew N. Kleiman, Comment, *The Right to Financial Privacy Versus Computerized Law Enforcement: A New Fight in an Old Battle*, 86 NW. U. L. REV. 1169, 1169-70 (1992) (observing courts, as opposed to legislature, were first to recognize right of privacy).

\textsuperscript{26} See Warren & Brandeis, *supra* note 1, at 193 (urging States should give some form of tort relief to persons whose private affairs were exploited by others); see also Grant, *supra* note 24, at 532 (discussing gradual development of privacy-related causes of action); William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 384-89 (1960) (stating same).

\textsuperscript{27} See *Roe*, 410 U.S. at 152-53 (1973) ("The Constitution does not explicitly mention any right of privacy. In a line of decisions, however, . . . the Court has recognized that a right of personal privacy, or a guarantee of certain areas or zones of privacy, does exist under the Constitution."); see also Bryan S. Schultz, Comment, *Electronic Money, Internet Commerce, And The Right To Financial Privacy: A Call For New Federal Guidelines*, 67 U. CIN. L. REV. 779, 787 (1999) ("[T]he United States Supreme Court did not begin to explore constitutional principles relating to privacy until the first half of the twentieth century."). *See generally* Bowers v. Hardwick, 478 U.S. 186 (1986) (deciding individual's right to privacy involving sexual and reproductive matters).

\textsuperscript{28} See, e.g., *Griswold*, 381 U.S. at 484-85 (holding that right of privacy exists under United States Constitution even though not expressly mentioned, but rather that "specific guarantees within the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance.").
In the landmark decision of *Katz v. United States*, the Supreme Court declared that an individual has a right of privacy whenever the individual has a "reasonable expectation of privacy." With respect to online commerce, there are several core "expectations or privacy" that individuals have long held that are now being invaded. Most of the invasions of privacy involve information privacy, which incorporates several privacy interests that are at times distinct and at times inextricable. Such interests include: the interest in preventing unauthorized access to personal information; the interest in preventing disclosure of information; the interest in ensuring accuracy of information; the freedom from observation of personal communications and anonymity. All of those privacy interests fall under the broad purview of "the right to be let alone" as articulated by Brandeis and Warren.

---

30 *Katz*, 389 U.S. at 359 (holding individual is entitled to privacy in public places, Justice Harlan's concurring opinion created current test for determining whether expectation of privacy is reasonable); see also *Katz*, 389 U.S. at 360-61 (Harlan, J., concurring) (establishing person must exhibit subjective expectation of privacy and society must recognize that expectation as reasonable); *Kelley v. Johnson*, 425 U.S. 238, 244-45 (1976) (involving individual's right as to personal appearance); *United States v. Miller*, 425 U.S. 435, 446-47 (1976) (involving individual's right of privacy in context of criminal investigation).
33 See McTigue, *supra* note 31, at 5 (stating reasonable expectation of privacy may be based on false perception of security and cyberspace anonymity); Pippin, *supra* note 7, at 128 (discussing personally identifiable information and its accessibility); Myrna L. Wigod, *Privacy in Public and Private E-Mail and On-line Systems*, 19 PACE L. REV. 95, (1998) (listing privacy interests that individuals have relating to Internet).
34 In their seminal piece on privacy, Warren and Brandeis state:

The protection afforded to thoughts, sentiments, and emotions, expressed through the medium of writing or of the arts...is merely an instance of the enforcement of the more general right of the individual to be let alone. It is like the right not to be assaulted or beaten, the right not to be imprisoned, the right not to be maliciously prosecuted, the right not to be defamed.

*See Warren & Brandeis, supra* note 1, at 205; *see also Kramer, supra* note 23 at 710-11
B. Privacy Rights And Commerce On The Internet

1. The origins of the Internet

The origins of the Internet date back to 1969 when the Department of Defense began developing a “robust computer network that would survive a nuclear attack on the United States.” Initially, the Internet remained relatively unknown and was utilized only by researchers, mathematicians, engineers, and computer experts. As the use of personal home computers heightened and Internet “browser” software was developed that allowed users to share and access information by linking various computer networks and made file transfer protocol easier to understand and utilize, the use of the Internet grew exponentially and terms such as “web-surfing” and “online commerce” have now become common vernacular.

2. Commerce on the Internet

The growth rate of the Internet is unprecedented in human history and its exponential growth is expected to continue well into the twenty-first century. Experts believe that within the next few years “billions of dollars will be poured into the

("the right to privacy is firmly ingrained in the common law of most states and occupies a prominent place in American society and jurisprudence."); Bieter, supra note 22 at 182 ("The makers of the Constitution appreciated that to civilized man, the most valuable of rights is the right to be let alone.").


36 See Baladi, supra note 35, at 252-53; Gladstone, supra note 6, at 1909 (noting Internet was initially for academics and government officials); Maureen A. O'Rourke, Fencing Cyberspace: Drawing Borders in a Virtual World, 82 MINN. L. REV. 609, 615 and n. 13 (1998) (describing origin of Internet).


38 See Tan, supra note 9, at 664 (noting that Internet use is expected to grow to approximately 320 million users worldwide by the year 2002).
Internet... with the expected return on investment in triple digits. Growing along with the Internet, although not at the same speed, is electronic commerce. Indeed, one of the principal forces driving the growth of the Internet is its position as a consumer marketplace.

Online commerce presents a completely new method of doing business that is neither dependent on geographic points of presence or chains of distribution. Because of the Internet's interactive, decentralized and open nature, commerce on the Internet is a multi-billion dollar industry. The electronic commerce industry is projected to grow to $717 billion by the end of 2001. With the advent of "virtual shopping malls" and other such online resources where users can easily make purchases from their computer, this growth is not surprising.

3. How privacy is being invaded on the Internet

As technological advances in the Internet have evolved, the fundamental right of privacy of the participants has been compromised. Web sites routinely gather data from visitors


40 See Topping, supra note 37, at 193 (discussing the growth rate of commerce on the Internet).

41 See Choppelas, supra note 31, at 344-46 (discussing effect of growth of on-line consumer market and its effects on growth of internet); see also Topping, supra note 37, at 193 (discussing growth rate of commerce on Internet).

42 See Berman & Mulligan, supra note 8, at 552 (discussing decentralized nature of internet and how it allows all users to 'publish' on it); see also Dan L. Burk, Federalism in Cyberspace, 28 CONN. L. REV. 1095, 1097 (1996) (discussing decentralized nature of Internet); David R. Johnson, The Rise of Law in Cyberspace, 48 STAN. L. REV. 1367, 1370 (1996) (discussing structure of internet).

43 See Gladstone, supra note 6, at 1907.


45 See Mark E. Budnitz, Privacy Protection for Consumer Transactions in Electronic Commerce: Why Self-Regulation Is Inadequate, 49 S.C. L. REV. 847, 852-55 (1998) (discussing how right of privacy has been compromised on Internet); Deborah McTigue, supra note 31, at 5 (1999) (discussing declining privacy rights since internet has become
overtly collecting information about the habits of their users. Recording, eavesdropping, collection and dissemination of private information can now be accomplished with incredible ease as the line between public and private realms has been blurred. Additionally, as a result of the unregulated nature of the Internet and the sophistication of the technology that supports it, information flows effortlessly from continent to continent making effective monitoring of the collection of data nearly impossible.

The Internet has hastened the trend of information collection by simultaneously facilitating the gathering of personal data, and, by its neural network ability to link immeasurable amounts of data to a particular individual, making the data more valuable. Web sites can extract information that the user does not voluntarily provide, such as the user's e-mail address, the type of browser being used and even the type of computer being used. Web sites can also obtain information through the use of "cookies" or "cookie files" which enable web sites to recognize a repeat visitor and track a specific individual's activities for the purpose of customizing content and advertising.


See Patricia Mell, Seeking Shade In a Land of Perpetual Sunlight: Privacy As Property in the Electronic Wilderness, 11 BERKELEY TECH. L.J. 1, 2 (Spring 1996) (noting that use of computers to manage information has blurred delineation between public and private realms); see also Pippin, supra note 7, at 125-26 (discussing lack of privacy on internet).

See Richard G. Barrows, Internet Ethics, 6 NEV. LAW. 18, 18 (June 1998) (discussing free flow of information on Internet); see also Hricik, supra note 37, at 463 (discussing how internet is not controlled by one distinct entity).

See Vern Countryman, The Diminishing Right Of Privacy: The Personal Dossier and the Computer, 49 TEX. L. REV. 837, 838 (1971) Professor Countryman asserts:

The computer has further facilitated the quest for efficiency. With its endless capacity to store data and to regurgitate it with lightening-like speed, it is inefficient not to use the computer to combine the various dossiers compiled on each individual. If the present trend continues, the day will come when the push of a button will produce a complete "data profile" on each citizen, from his departure from the womb (or perhaps sometimes earlier) to some time after he enters his tomb.

Id. at 838.

See Elizabeth deGrazia Blumenfeld, Privacy Please: Will The Internet Industry Act To Protect Consumer Privacy Before The Government Steps In?, 54 BUS. LAW. 349, 350 (Nov. 1998) (discussing ease of access to consumer information on internet).

See Belgium, supra note 5, at 1 n.21 (discussing server's use of cookie technology to track preferences of users); see also Jerry Kang, Information Privacy in Cyberspace Transactions, 50 STAN. L. REV. 1193, 1227-28 (1998) (discussing use of cookies by servers).
That transactional data, also known as "mouse droppings" or clickstream data, may then be sorted and reused. This repository of digital fingerprints reveals the blueprint of the consumer, known as a user profile, and can be stored, aggregated and analyzed to provide a rich source of information that can later be used by the website sponsor or sold for profit.

4. Who is violating our right to privacy and why they are doing it

When examining who is violating our right to privacy, it becomes clear that the answer is just about everybody. It is estimated that an astonishing ninety-two percent of websites collect personal data. To be sure, one recent industry-funded survey, which involved 361 websites drawn from the busiest 7,500 servers on the Internet, found that 93 percent of those sites collected personal information. Interestingly, the gathering

51 See Peter McGrath, Knowing You All Too Well, NEWSWEEK, Mar. 29, 1999, at 48 (discussing recording web movement of users through clickstream data); see also MICROSOFT PRESS COMPUTER DICTIONARY 286 (3d ed. 1997) (defining clickstream data).

52 See Belgum, supra note 5, at 79 ("Profiling is the term used to denote the gathering, assembling, and collating of data about individuals in databases which can be used to identify, segregate, categorize and generally make decisions about individuals known to the decision-maker only through their computerized profile.").

53 See Belgum, supra note 5, at 79 (defining profiling); see also Charles F. Luce, Jr., Internet Privacy: Spam And Cookies: How To Avoid Indigestion While Binging At The World Wide Automat, 27 COLO. LAW. 27, 30 (Oct. 1998) ("The perceived danger to privacy lies in the possibility of a website combining cookie data with registration data and then pooling this data with other data to compile a detailed profile of user tastes based on online activities.").

54 See Mark E. Budnitz, Privacy Protection for Consumer Transactions in Electronic Commerce: Why Self-Regulation is Inadequate, 49 S.C. L. REV. 847, 859 (1998) (discussing how businesses are covertly collecting information about consumers without consent); see also Anne Meredith Fulton, Cyberspace And The Internet: Who Will Be The Privacy Police?, 3 COMM. LAW CONSPECTUS 63, 64 (Winter 1995) (discussing private nature of internet as source of possible rampant abuse).

55 See FTC, Privacy Online: A Report To Congress (June 1998) (visited October 11, 2001) (reporting ninety-two percent of 1,402 websites surveyed collected some personal data); see also Pippin, supra note 7, at 125 (concluding presence of privacy policy statements does little to safeguard Internet user's privacy). See generally Jane E. Prine, Torts – No Longer Living In A Glass House: Every Minnesotan is Entitled to a Right To Privacy, 25 WM. MITCHELL L. REV. 999, 1015 (1999) (stating benefits of these technological devices have detrimental effects on person's right to privacy).

56 See Mary J. Culnan, Georgetown Internet Privacy Policy Survey: Report to the Federal Trade Commission (last modified August 11, 2000) (reporting results of survey conducted to provide progress report to FTC on extent to which commercial websites have posted privacy disclosures); see also Christine A. Varney, Consumer Privacy in the Information Age: A View from the United States, 505 PL/PAT 629, 634 (1996) (stating
and dissemination of personal information for profit is not limited to the private sector as the government has been making substantial sums of money from the sale of personal information of years.57

The reasons why those various groups collect personal information are legion. But without a doubt the foremost motivation is for financial gain. The current market for personal information is a whopping $1.5 billion per annum.58 Moreover, it appears that the online information collection industry has a bright future “as economic success in industry becomes more dependent upon having greater quantities and better quality information.”59

that personal information is being collected at rate and to degree unthinkable even five years ago. See generally Tya Turner, AT&T Sets New Privacy Model, TECH WEB NEWS, September 24, 1998 (explaining how AT&T has revised its online privacy policies to reassure customers that personal information will remain within confines of AT&T).

57 See Nina Berstein, On line, High-Tech Sleuths Find Private Facts, N.Y. TIMES, Sept. 15, 1997, at A20 (reporting both state and federal governments have used sale of personal data to boost revenues, specifically Illinois’ approximate ten million dollar annual revenue from sale of private records); see also John Caher, Senate Task Force Aims to Protect Citizens Privacy, ALBANY TIMES UNION, February 10, 1999 at B2, (explaining that New York collects more than forty-nine million dollars by selling information on motorists); see, e.g., Erika S. Koster, Zero Privacy: Personal Data on the Internet, THE COMPUTER LAWYER, May 1999, at 7 (stating United States Postal Service is also guilty of selling private information by listing of 108 million permanent change-of-address cards filed by relocating postal clients to direct marketers).

58 See Joel R. Reidenberg, Restoring Americans’ Privacy in Electronic Commerce, 14 BERKELEY TECH. L.J. 771, 776 (Spring 1999) (explaining that companies such as Axcioin and First Data are two such data collection companies that sell information personal information such as ethnic or religious affiliations and even whether a person buys a particular type of underwear); see also In the Matter of Trans Union Corporation, FTC Docket No. 9255, at 53 (July 31, 1998), <http:/www.ftc.gov/os/198/9898/d9255pub.id.pdf> (“Five companies’ revenues represent 40% of this $1.5 billion market: R.L. Polk & Company, ACXIOM, Metromail Corporation, First Data Solutions and ABI/DBA”). See generally Blumenfeld, supra note 49, at 349 n.14 (arguing there are two ways in which web site can collect personal consumer information: overtly and clandestinely).

59 See Gladstone, supra note 6, at 1923 (“The electronic commerce industry for information will continue to expand as economic success in society becomes more dependent upon having greater quantities and better quality information”); see also Bob Tedeschi, Targeted Marketing Confronts Privacy Concerns, N.Y. TIMES ON THE WEB, May 10, 1999 (reporting assessment by electronic commerce industry analyst that “[t]he trend toward capturing and using information is the future of online commerce.”); Pippin, supra note 7, at 126 (“The internet, and specifically the World Wide Web, has become a primary source for obtaining goods, services, and information by a large number of people in a very short period of time”).
5. The importance of protecting the right of privacy in online commercial transactions

Implementing effective safeguards to protect against abuses in online commercial transactions is critical to the success of Internet commerce.\(^\text{60}\) Even though public disclosure of personal data is a phenomenon that pre-dates the advent of the computer,\(^\text{61}\) with the creation of the Internet, and its prevalence in today's society, threats of invasion of privacy, both real and perceived, have risen to another level.\(^\text{62}\) Those threats have greatly hindered the growth of online commerce and the Internet itself.\(^\text{63}\) In fact, the foremost reason given by individuals for refusing to use the Internet was not its cost or technical complexity, rather it was because of privacy issues.\(^\text{64}\) Of those

\(^{60}\) See David W. Koch and Meredith Fuchs, Franchisor Survival Guide to Online Privacy, What Hath Technology Wrought?, 19 FRANCHISE L.J. 47, 47 (Fall 1999) (stating that in short period of time, Internet privacy has become significant public concern); see also Budnitz, supra note 54, at 849 (finding in 1997 Harris survey that majority of consumers engaging in online activities and Internet transactions are worried about confidentiality and security of these systems); see, e.g., Margaret Jane Radin and Daniel L. Appelman, Doing Business In the Digital Era: Some Basic Issues, 570 PLI/PAT 51, 62 (August/September 1999) (explaining how people are worried that if this kind of information gathering and marketing goes unchecked, everyone who uses credit card or browses online will be open book).

\(^{61}\) See Whalen v. Roe, 429 U.S. 589, 603-04 (1977) (holding that State of New York had right to collect names and addresses of all who had purchased prescription drugs); see also Lamont v. Commissioner of Motor Vehicles, 269 F. Supp. 880, 884 (S.D.N.Y. 1967), aff'd, 386 F.2d 449, 450 (2d Cir. 1967) (holding that statute allowing collection and disclosure of addresses and telephone numbers of driver's license holders did not constitute "substantial" violation of privacy rights); Shibley v. Time, Inc., 341 N.E.2d 337, 341 (Ohio Ct. App. 1975) (allowing sale of publisher's subscription list to direct marketer).

\(^{62}\) See Pippin, supra note 7, at 126-27 (stating hesitation of consumers to conduct online purchasing is uncertainties over how laws and regulations in existence before emergence of Internet actually apply to Internet commerce, if at all); see also, Hammond, supra note 4, at 102 (finding that 61% of people surveyed would be more likely to start using internet if privacy of their personal information and communication would be protected). But see Varney supra note 56, at 631 (pointing out there is no law or regulation that establishes citizen's right to informational privacy in United States).

\(^{63}\) See Gladstone, supra note 6, at 1908 (concluding there is consensus among various industry experts that consumer's desire to be anonymous, or at least unexposed, to unknown parties has tempered growth of Internet commerce); see, e.g., Budnitz, supra note 54, at 850-51 (showing that percentage of American households connected to Internet has doubled in last two years but despite this promising potential market, if consumers do not trust companies to protect their privacy then companies will generate enough volume to be profitable).

\(^{64}\) See Hammonds, supra note 4, at 102 (surveying 999 adults and concluding top reason people are staying off web is to protect their personal information); see also Budnitz, supra note 54, at 848-49 (finding consumers believe that electronic commerce systems are capable of invading their privacy and stealing information and this plays significant factor in consumers' resistance to participate).
individuals using the Internet, seventy-eight percent stated that they would use it more if their privacy were guaranteed.\textsuperscript{65}

The potential economic impact of widespread commercial use of the Internet is astounding. But as the Internet continues to evolve as a commercial marketplace, Internet privacy will remain the primary concern of consumers or potential consumers until effective measures are taken.\textsuperscript{66} The development and implementation of broad privacy protection, therefore, is vital in terms of fostering the commercial uses of the Internet.\textsuperscript{67}

III. CURRENT INADEQUATE ONLINE PRIVACY PROTECTIONS

Today there is no comprehensive protection for personal information in the United States. Commercial web sites are generally responsible for voluntary compliance or self-regulation concerning consumer privacy and fair information practices online. In the absence of any comprehensive legislation, it is necessary to apply traditional state and federal statutes, caselaw, regulations and the nebulous "penumbras" of privacy inherent in the Bill of Rights to consumer transactions on the Internet. But "[a]pplying existing legal and regulatory paradigms to the Internet seems to be unavailing."\textsuperscript{68} There is much confusion as

\textsuperscript{65} See Hammonds, supra note 4, at 102.

\textsuperscript{66} See Gladstone, supra note 6, at 1918 (stating that statutory and self-regulatory mechanisms designed to protect transactional privacy of Internet users have not been successful); see also Hammonds, supra note 4, at 102 (noting results of survey conducted in 1998 showing that consumers not currently using Internet ranked concerns about privacy and communications as biggest reasons they do not use Internet).

\textsuperscript{67} See Reidenberg, supra note 58, at 771 ("Privacy is a critical issue for the growth of electronic commerce."); Schultz, supra note 27, at 799 ("The existence of broad privacy protection is particularly important in terms of furthering commercial uses of the Internet."); see also Spiros Simitis, Reviewing Privacy In An Information Society, 135 U. PA. L. REV. 707, 738 (1987).

[Government as well as private enterprises have, for far too long, considered the use of personal data to be the norm. Instead of asking how to perform their task without resorting to personal information, their interest has concentrated on developing new and better retrieval methods. Advances in processing have become synonymous with easier and quicker access to a steadily growing amount of data usable for more and more purposes. Consequently, where a "convenient" use of computers appears to be the sole concern, purely technocratic considerations have held sway over all others.

\textsuperscript{Id.} at 738 (footnote omitted).

\textsuperscript{68} Topping, supra note 37, at 189; see also H. Joseph Hameline and William Miles, The Dormant Commerce Clause Meets the Internet, 41 B.B.J. 8, 8 (September/October 1997) (examining dormant Commerce Clause and how it is becoming important legal doctrine at intersection of state law and Internet); see, e.g., United States v. Christopher
to whether those protections provide any level of informational privacy protection on the Internet due to a number of factors not the least of which is the difficulty associated with applying traditional terminology to modern Internet practice. The following is a brief description of the online privacy protections currently in place that are arguably applicable to online commerce and the reasons why those protections are inadequate.

A. Self-Regulation

Due to the government’s lack of desire to provide effective regulation with regard to online informational privacy, the United States currently follows a policy of self-regulation whereby Internet users and operators set the rules and regulations. Not surprisingly, this approach has been resoundingly endorsed by “key Internet players.” But allowing the industry to regulate itself has been aptly described as like “the fox watching the hen house.” Notwithstanding the inherent benefits of a medium free from government interference, it is abundantly clear that the current relaxed self-regulatory structure is simply not working and legislation is needed.

B. Carroll, 105 F.3d 740, 742 (1997) (stating that Internet is equivalent to moving photographs across state lines and this constitutes transportation in interstate commerce).

See Fulton, supra note 54, at 64 (“The rapid growth of computer technology has left the law in the dust. There are limited laws regulating Cyberspace, and many of its users and program activities remain unchecked.”). But see FTC, supra note 55, at <http://www.ftc.gov/reports/privacy/3/exeintro.htm> (explaining that several regulatory initiatives have been formed to protect overall privacy interests of individuals that use Internet).

See Gladstone, supra note 6, at 1916 (noting that government’s laissez-fair approach to regulating Internet by allowing private sector to take lead has been endorsed by Internet community); see, e.g., Topping supra note 68, at 181 (explaining framework of Internet Tax Freedom Act that was signed into law by President Clinton in 1998 which addresses economic potential of Internet and endorsed its lack of legal framework).

Id. at 131 (stating that skeptics of governmental intervention contend that “the local, state, and federal government are all incapable of implementing effective rules and enforcement mechanisms, due partially to the speed at which technology is advancing”) (footnote omitted); see also David W. Carney, Online Privacy Bill Runs Aground, TECHNOLOGY LAW JOURNAL (July 27, 1999) <http://www.techlawjournal.com/privacy/19990727.htm> (quoting from Senator John McCain, Chairman of the Commerce Committee, “[I]n fact, regulation could impede development and deployment of new technology that may empower consumers to protect their own privacy.”)

See Pippin, supra note 7, at 133 (stating that “[w]ith so many different approaches
In order to stave-off federal regulation many prominent Internet companies have already implemented policies designed to increase consumer confidence. Additionally, various privacy self-regulation organizations have been created to address the issue. For instance, in 1998, the Commerce Department and The National Telecommunications and Information Administration, which advises the Secretary of Commerce and the President of the United States on domestic and international communications issues, jointly released a discussion draft of a report entitled "Elements of Effective Self-Regulation for Protection of Privacy" (the "Report"). The Report recommended that online consumers should be informed of the identity of the collectors of personal information and the intended use of the information. The Report also recommended that businesses to the problem of Internet privacy, self-regulation has not yet proven to be the best possible solution.

See Stephen J. Davidson & Katheryn A. Andersen, The UCITA Revolution: The New E-Commerce Model for Software and Database Licensing, 600 PLI/PAT 553, 561 (April/May 2000) (describing Better Business Bureau's creation of certification program for Internet businesses' privacy programs, which guarantees consumers that such programs provide appropriate privacy safeguards); Radin & Appelman, supra note 60, at 64 (noting that important Internet sites are promulgating privacy policies in hope of avoiding federal or state regulation); Domingo R. Tan, supra note 9, at 674 & n.84 (listing Adobe, BPI Communications, CBS, CNET, Collier Newfield, ConEx, Digimarc, MSNBC, Playboy Enterprises New Media Group, Sony On-line Ventures, IBM, AT&T, and the New York Times as companies using their own seals of approval to promote consumer confidence in on-line transactions).


See 63 FED. REG. 30,729 (June 5, 1998).

See 63 FED. REG. 30,731; see also Lee S. Adams & David J. Martz, Development in Stored-Value Cards and Cyberbanking, 54 BUS. LAW. 1373, 1383 (1999) (Report recommends self-regulatory procedures enable consumers to choose how personal information is used); Belgum, supra note 5, at 65 (citing Report as requiring “Awareness”

2002] PRIVACY IN INTERNET COMMERCE 409
provide consumers with the opportunity to choose whether and how their personal information is used. But the government never implemented the proposals set forth in the Report.

Recently, however, on July 27, 2000, the Federal Trade Commission ("FTC") voted 4-1 to endorse a self-regulatory plan submitted by the Network Advertising Initiative ("NAI"), a consortium comprised of more than 90 percent of Internet advertising companies. The self-regulatory plan requires advertising companies on the Internet to detail their data collection policies and give consumers the opportunity to opt-out of data collection efforts. The advertising companies also promised to give consumers "reasonable access" to personally identifiable information collected about them and to make "reasonable efforts" to protect the data they collect.

But privacy advocates immediately criticized the self-regulatory plan stating that it does not go far enough to ensure that personal information collected online about consumers will not be misused because it places the burden on the consumer to "opt-out" of the data collection procedures, it fails to provide for any penalty if companies fail to follow the guidelines and it fails to guarantee compliance by advertising firms that are not

or disclosure of identity of data collecting party and means for avoiding participating in such transactions).

78 See 63 FED. REG. 30,731 see also Belgium, supra note 5, at 65 (citing Report as requiring "Choice," or mechanism to exercise options such as "affirmative choice" for certain "sensitive" categories of information); Scott Killingsworth, Minding Your Own Business: Privacy Policies in Principle and in Practice, 7 J. INTELL. PROP. L. 57, 68 (1999) (citing Report as articulating elements of "Fair Information Practices" which represent consensus approach to personal information privacy that allows consumers to participate in decisions on disclosure and use of personal information).


80 See Schecter & Muhlbach, supra note 79, at 756-57 (stating NAI Plan requires user to exercise choice of how personal information is used for purposes unrelated to its collection, and that user is given, at a minimum, choice to opt-out); Polonetsky, supra note 79, at 792 (identifying NAI's requirement of posting detailed data collection policies and making available opt-out policies).

81 See Schecter & Muhlbach, supra note 79, at 747 (stating NAI Plan requires advertisers to establish mechanisms such as consumer access and use of reliable sources to assure accuracy of personal information; see also Polonetsky, supra note 79, at 800 (stating NAI Plan requires advertisers to make "reasonable efforts" to protect the data they collect for OPM from loss, misuse, alteration, destruction or improper access).
members of the NAI. While the FTC never stated that the Network Advertising Initiative is the privacy model the FTC seeks for all online commerce, "federal officials have suggested that it comes close." 83

Although certain online businesses and reform groups have established, or promise to establish, their own privacy guidelines, the government, Internet users, and numerous online businesses agree that self-regulation has failed. 84 Even the FTC, on the very same day it approved and publicly supported the NAI's self-regulatory plan, announced that it still intended to pursue privacy legislation in Congress. 85 Because of the inherent shortcomings of self-regulation and the apparent need for new legislation, it is plainly a question of whether or not the government is willing to follow through with its threat of intervention.

82 See Jessica Melugin, Double-Click for Consumers, WASHINGTON TIMES, August 1, 2000, at A18 (noting consumers' absence from negotiating table results in lack of benefits to consumers); Striking The Wrong Balance, BUFFALO NEWS, Aug. 14, 2000, at B2 (arguing FTC has sold out public while caving into marketers in endorsing "anemic" plan to govern online privacy); see also Good News Monday; Privacy - Online Protections, CINCINNATI ENQUIRER, July 31, 2000, at A10 ("While [the Network Advertising Initiative is] looking in the right direction, it doesn't go far enough to give consumers truly informed choices," quoting Ari Schwartz of Center for Democracy and Technology); John Solomon, FTC Backs Privacy Plan for Net Users: Advertisers Will Self-Regulate Web Profiling, CHICAGO TIMES, July 28, 2000, at B1 (recognizing privacy advocates' fear of misuse or transmission of gathered information to third parties without online users' consent).


84 See Reidenberg, supra note 58, at 776 (noting U.S. government's recognition of hypothetical self-regulation in corporate America); Trubow, supra note 9, at 832 (stating internet users have reached consensus that self-regulation is not enough); Eric J. Sinrod et al., Comment, The New Wave of Speech and Privacy Developments in Cyberspace, 21 HASTINGS COMM. & ENT. L.J. 583, 598 (1999) (noting civil rights and privacy organizations' skepticism of industry efforts at self-regulation); Gladstone, supra note 6, at 1918 (asserting "The evidence suggests that the statutory and self-regulatory mechanisms designed to protect the transactional privacy of Internet users have not yet been successful").

85 See Ramey, supra note 83, at 2; E-Commerce/Technology, supra note 83, at 2 (noting FTC's approval of NAI's "guidelines," but also noting FTC's recent report communicating need for legislation to protect consumers).
B. Constitutional Protections

1. The United States Constitution

There are two amendments to the United States Constitution that indirectly address privacy issues relating to online commerce—The First Amendment which prohibits laws abridging the freedom of speech, assembly, or the press; and the Fourth Amendment which protects people from unreasonable government intrusion. But privacy protections provided by the Constitution are limited by the state action requirement of the Fourteenth Amendment. Under the state action requirement, the constraints on access to information imposed by the Constitution only apply to governmental entities and not to the private sector. Thus, the Constitution protects a citizen's right of privacy from unlawful intrusion by the government, but does not protect citizens from privacy invasions committed by private citizens.

See infra nn. 87-99 & accompanying text (discussing First and Fourteenth Amendments of U.S. Constitution); see also U.S. CONST. amend. I (providing Freedom of Speech and Freedom of Press); U.S. CONST. amend. XIV, § 1 (Due Process and Equal Protection Clauses).

See U.S. CONST. amend. XIV, § 1 (providing, in pertinent part "nor shall any state deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws") (emphasis added); see also Shelley Ross Saxer, Shelley v. Kraemer's Fiftieth Anniversary: "A Time For Keeping, A Time for Throwing Away?" 47 U. KAN. L. REV. 61, 62-63 (1998) (arguing private racial discrimination be addressed using alternatives to state action doctrine such as public policy, balancing of conflicting rights, and legislative enactments to prevent further clouding line between state and private action). See generally Kevin L. Cole, Federal and State "State Action": The Undercritical Embrace of a Hypercriticized Doctrine, 24 GA. L. REV. 327, 328-30 (1990) (further discussing "state action" doctrine from both state and federal perspective).

See Jackson v. Metro. Edison Co., 419 U.S. 345, 349 (1974) (noting Fourteenth Amendment provides "essential dichotomy ... between deprivation by the State, subject to scrutiny under its provisions, and private conduct, however discriminatory or wrongful, against which the Fourteenth Amendment offers no shield"); Shelley v. Kraemer, 334 U.S. 1, 13 (1948) (noting Fourteenth Amendment erects no shield against merely private conduct, however discriminatory or wrongful); see also Lugar v. Edmonson Oil Co., 457 U.S. 922, 937 (1982) (laying out two-part test for determining state action: first, deprivation must be caused by exercise of some right or privilege created by State or by rule of conduct imposed by State or by person for whom State is responsible; and second, party charged with deprivation must be person who is clearly a State actor).

See Robert J. Glennon & John E. Nowak, A Functional Analysis of the Fourteenth Amendment "State Action" Requirement, 1976 SUP. CT. REV. 221, 232-33 (1976); Saxer, supra note 84, at 61-62 (characterizing Shelley v. Kraemer decision as blurring line between state action which is subject to constitutional restrictions, and private action which is not). See generally Cole, supra note 87, at 330 (1990) (further discussing "state
The First Amendment, which limits the government’s power to collect data where the government’s involvement would interfere with the ability to publish or distribute speech, provides some level of informational privacy regarding defamatory speech.\textsuperscript{90} The First Amendment, as it relates to defamation, has little applicability in online privacy because most of the private information that is disclosed to commercial web sites is true, thus negating the element of falsity required by defamation statutes.\textsuperscript{91} Additionally, in \textit{New York Times Co. v. Sullivan},\textsuperscript{92} the United States Supreme Court held that for a public official to prevail in a defamation suit, the public figure must demonstrate that the statement is false and was made with actual malice.\textsuperscript{93} As such, the Court severely limited the applicability of common law privacy torts in cases involving newsworthy individuals.\textsuperscript{94}


\textsuperscript{91} \textit{Compare} CAL. CIV. CODE 45 (West 2000) (defining libel as “a false and unprivileged publication by writing, printing, picture, effigy, or other fixed representation to the eye, which exposes any person to hatred, contempt, ridicule, or obloquy, or which causes him to be shunned or avoided, or which has a tendency to injure him in his occupation) (emphasis added) \textit{and} GA. CODE ANN. 45 (West 2000) (defining libel as “a false and malicious defamation of expressed in print, writing, pictures, or signs, tending to injure the reputation of the person and exposing him to public hatred, contempt, or ridicule) (emphasis added), with N. Y. CONST. art. 1 (providing, in pertinent part, “[I]n all criminal prosecutions or indictments for libels, ...if it shall appear to the jury that the matter charged as libelous is true, and was published with good motives and for justifiable ends, the party shall be acquitted.”) (emphasis added). \textit{But see} Rhonda G. Hartman, 71 OR. L. REV. 855, 874 (1992) (stating “[w]hen private speech threatens civility of a society directly...or indirectly, as through discriminatory acts injurious to reputation or privacy, the threat of deleterious effect arguably need not be tolerated; defamatory...speech should not be allowed to ‘demean the grand conception of the First Amendment,” quoting \textit{Miller v. California}, 413 U.S. 15, 34 (1973)).

\textsuperscript{92} 376 U.S. 254 (1964).


\textsuperscript{94} \textit{See} \textit{Sullivan}, 376 U.S. at 283 (requiring actual malice); \textit{see also} John J. Walsh, \textit{Damages: Will They Be Different in the New Millennium?}, 523 PLJ/PAT 297, 304 (1998).
Therefore, "the First Amendment provides little, if any, privacy protection for personal information collected by web site operators." 95

The Fourth Amendment also provides only limited protections against the invasion of privacy. 96 The Supreme Court first recognized a constitutional right for information privacy in Whalen v. Roe. 97 In this 1977 case, the Court upheld a state statute that required doctors to disclose information to the state on individuals taking certain highly addictive prescription drugs for inclusion on a state database. 98 Although the Court upheld the statute, it affirmed an individual's right to have his personal information protected by the government stating that "[b]road dissemination by state officials of such information, however, would clearly implicate constitutionally protected privacy rights . . . ." 99

Even though the Supreme Court recognized a Constitutional right to informational privacy, it has repeatedly noted the absence of constitutional protection for information that individuals place into the flow of commerce or otherwise


96 The Fourth Amendment to the U.S. Constitution is as follows:

The right of the people to be secure in their persons, house, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. CONST. amend. IV.


98 Id.

99 Id. at 606. The Whalen Court also held with respect to an individual's right to privacy protection from the government:

We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files. The collection of taxes, the distribution of welfare and social security benefits, the supervision of public health, the direction of our Armed Forces, and the enforcement of the criminal laws all require the orderly preservation of great quantities of information, much of which is personal in character and potentially embarrassing or harmful if disclosed. The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures.
voluntarily disclose. Although it certainly can be argued that online users have certain privacy interests in the online world even when voluntarily disclosing private information, as the United States Supreme Court held in *Katz*, the Fourth Amendment "protects people not places." In other words, what a person knowingly exposes to the public, even in his own home or office, is not subject to Fourth Amendment protection. Consequently, the Supreme Court's decision in *Katz* and its progeny leads to the conclusion that the Fourth Amendment does not apply to protect online consumers from the dissemination of their private information because they voluntarily exposed that information to the public.

2. State constitutional privacy protections

Like the United States Constitution, the great majority of state constitutions do not expressly provide a right to privacy although they do offer protections against unreasonable searches and seizures. However, judicial interpretations of those state constitutional provisions, like those interpreting the United States Constitution, have limited the privacy right to protect only against government intrusions. Also, states are severely hampered in their efforts to protect the privacy of individuals engaging in interstate commerce because of the Internet's

100 *See United States v. Miller*, 425 U. S. 435, 442-47 (1976) (holding that there is no expectation of privacy when bank discloses customer's records after being served with subpoena); *Smith v. Maryland*, 442 U. S. 735, 742 (1979) (holding that there is no expectation of privacy for phone records dialed into telephone); *see also* *Rakas v. Illinois*, 439 U.S. 128, (1978) (reiterating that one who voluntarily discloses something to another assumes risk of losing Fourth Amendment protection).


105 *Id. See United States v. Gori*, 230 F. 3d 44, 50 (outlining Supreme Court's historical limitations on privacy rights).
inherently a-jurisdictional nature that makes acquiring jurisdiction to impose sanctions on violators difficult if not impossible.106

C. Federal Information Privacy Statutes

Although the United States does not have an omnibus law that governs the treatment of personal information over the Internet, Congress has passed certain federal statutes and regulations to control the collection, use and dissemination of information in particular industries. Nevertheless, only a few of those statutes afford any protection to online consumers. The primary federal statutes that may be interpreted as providing some level of privacy protection to online consumers are the Electronic Communications Privacy Act of 1986107 and the Fair Credit Reporting Act.108 Several other federal statutes may also play a minor role in safeguarding the rights of online consumers, but none provide the broad legislation needed to halt, or at least curtail, the involuntary collection and use of personal information in online commercial transactions.

1. The Electronic Communications Privacy Act of 1986

In an effort to address the privacy concerns attendant to newly developing electronic technology, Congress passed the Electronic Communications Privacy Act of 1986 ("ECPA").109 The ECPA is currently the only federal statute that specifically addresses

106 See Henry H. Perritt, Jr., Jurisdiction in Cyberspace, 41 VILL. L. REV. 1, 2-3 (1996) ("Conventional doctrines of jurisdiction to prescribe, to adjudicate and to enforce legal decisions must evolve to handle new disputes in cyberspace."); John A. Lowther IV, Comment, Personal Jurisdiction and the Internet Quagmire: Amputating Judicially Created Long-Arms, 35 SAN DIEGO L. REV. 619, 653 (1998) ("Our ancient and outdated notions of geography, territory, and presence have finally met their match against an entity that has no geography, is not confined to any one territory, and gives everyone an instant presence everywhere.").
interception and access of electronic communications. The ECPA prohibits unauthorized access, interception or disclosure of electronic communications\(^\text{110}\) including data transmissions between computers, pagers, e-mail and video transmissions.\(^\text{111}\) The ECPA is a complex statute that provides important privacy protections because it imposes harsh penalties, both criminal\(^\text{112}\) and civil,\(^\text{113}\) for violation of the statute.\(^\text{114}\)

But the ability of the ECPA to provide protection in the online commercial realm is uncertain because the government has heretofore been reluctant to bring such suits under the statute.\(^\text{115}\) Furthermore, the breadth of the ECPA is not sufficient to protect all forms of online information abuse. For instance, because the ECPA only extends to the contents of communications, transactional information associated with electronic communications, such as the existence of communications, identities of the parties, the length of the message, duration of the communication and the length of the message are not protected.\(^\text{116}\) Additionally, the ECPA is mostly

\(^{110}\) See 18 U.S.C. § 2510(12) (1994) (defining electronic communication as “any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce. . . . “).

\(^{111}\) See 18 U.S.C. § 2510.


\(^{114}\) See 18 U.S.C. §§ 2511, 2520, 2701, 2707 (1994); see also Miller, supra note 109, at 460 (stating same); Shubert, supra note 109, at 402 (stating same).


\(^{116}\) See 18 U.S.C. §§ 2520, 2521, 2707 (1986). A service provider is, however, prohibited from knowingly divulging the contents of the communication. See 18 U.S.C. §2702(a)(1). This distinction between context and content is important in understanding the scope of the ECPA. See also Miller, supra note 109, at 461-62 (stating that although EPCA regulates disclosure of contents of electronic message, it “does not prohibit disclosure of information unrelated to the content of the message”).
limited to communications stored for less than 180 days.\textsuperscript{117} Thus, although the ECPA provides significant privacy protection to certain types of electronic transactions, its limited scope severely limits its applicability to the information abuse problems now faced by online consumers.

2. The Fair Credit Reporting Act

Another piece of legislation that may provide some privacy protection to online consumers is the Fair Credit Reporting Act ("FCRA"), which establishes important privacy protections for consumers' sensitive financial information by governing the ability of consumer credit reporting agencies to disclose personal information in supplying credit information.\textsuperscript{118}

The FCRA is important to the online consumer because credit report information is becoming increasingly accessible on the Internet as more users make online purchases with their credit cards.\textsuperscript{119} The FCRA restricts the disclosure of consumer credit reports and other personal information to entities with particular "permissible purposes," such as eligibility for personal credit or insurance, employment purposes, and licensing.\textsuperscript{120} The FCRA

\begin{footnotesize}
\begin{enumerate}
  \item See 18 U.S.C. § 2703(a); Schultz, supra note 111, at 796, (NEED PARA). But see Michael S. Leib, Email and Wiretap Laws: Why Congress Should Add Electronic Communication to Title III Statutory Exclusionary Rule and Expressly Reject a Good Faith Exception, 34 HARv. J. ON LEGIS. 393, 405-07 (1997) (stating that government may obtain communication stored for more than 180 days through warrant, administrative subpoena, grand subpoena, or court order).
  \item See Gladstone, supra note 6, at 1909. When purchasing goods or services over the Internet by credit card, the customer must either e-mail his credit card/personal identification details to the merchant or enter the credit card information on the merchant's web page thereby necessarily exposing private information. Id. Making an online purchase with cash provides the most privacy protection during an online transaction as it is fungible, largely untraceable and no additional assurance of authenticity is needed. However, making a payment by cash presents other obvious obstacles such as the need for an instantaneous method of payment.
  \item See 15 U.S.C. § 1681(e). The FCRA provides in relevant part: Every consumer reporting agency shall maintain reasonable procedures designed to avoid violations of § 1681(c) of this title and to limit the furnishing of consumer reports to the purposes listed under § 1681(b) of this title. These procedures shall require that prospective users of the information identify themselves, certify the purposes for which the information is sought, and certify that the information will be used for no other purpose. Every consumer reporting agency shall make a reasonable effort to verify the
\end{enumerate}
\end{footnotesize}
provides compensatory damages and attorneys' fees for negligent noncompliance and punitive damages for willful noncompliance. The FTC is endowed with the administrative powers to enforce the FCRA pursuant to the Federal Trade Commission Act.

The authority granted under the FCRA has been limited, however, by the courts' interpretation of a "consumer report." For example, in Trans Union Corp. v. FTC, the United States Court of Appeals for the D.C. Circuit overturned an FTC order that Trans Union Corporation's sale of "targeted marketing" mailing lists was a consumer report for an impermissible purpose under the FCRA. The FTC contended that the mailing lists

identity of a new prospective user and the uses certified by such prospective user prior to furnishing such user a consumer report. No consumer reporting agency may furnish a consumer report to any person if it has reasonable grounds for believing that the consumer report will not be used for a purpose listed in § 1681(b) of this title.

Under the FCRA, a consumer report is defined as:

Any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for (a) credit or insurance, (b) employment purposes or (c) any other purpose authorized under § 1681(b).

See 15 U.S.C. § 1681(a) & (n). See Thornton v. Equifax, Inc., 619 F. 2d 700, 703 (1980) (stating that FCRA provides when violations of statute are willful, damages recovered can be actual and punitive, and plaintiff may also recover attorney fees); Mangio v. Equifax, 887 F. Supp. 283, 284 (1995) (stating that individuals may sue for damages if credit agency willfully fails to comply with its FCRA obligations, rendering agency liable to individual for his or her actual damages as court will allow).

See 15 U.S.C. § 1681(s); see also Mangio, 887 F. Supp. at 285 (stating that Congress granted FTC power to sue individual creditors for injunctive relief; under FCRA's administrative enforcement provision, credit agencies "compliance" with FCRA shall be enforced by FTC. Violations of FCRA constitute unfair or deceptive acts under FTCA).

Under the FCRA, a consumer report is defined as:

Any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for (a) credit or insurance, (b) employment purposes or (c) any other purpose authorized under § 1681(b).


See Trans Union, 81 F. 3d at 228 (D.C. Cir. 1996).

See Trans Union, 81 F. 3d at 229 (PARA); Hovater, 823 F. 2d at 418 (explaining that FCRA limits permissible purposes to occasions when agency is subject to court order, acting with consent of consumer, or performing service for agency who reasonably believes that information is to be used to determine eligibility for insurance, credit, license or other governmental instrumentality, for employment purposes or other legitimate business purpose); see Heath v. Credit Bureau of Sheridan, Inc., 618 F. 2d 693, 696 (YEAR) (stating that pursuant to statute, permitted purposes to which protected information must relate, must be about consumer transaction, and therefore information not supplied to person not engaged in such transaction cannot be consumer report).
were consumer reports because they were compiled using credit account data. The Trans Union court held that the mailing lists were not consumer reports because the “implicit information conveyed therein” was not collected “to serve as a factor in determining credit eligibility.” The narrow interpretation of what constitutes a “consumer report” by the courts has severely limited the applicability of the FCRA. Furthermore, under the FCRA, agencies are not required to notify individuals of the existence, content, or use of financial records. “Thus, the FCRA provides little privacy protection” to online consumers.

3. Other federal privacy legislation

Other federal acts protecting informational privacy include: the Computer Fraud and Abuse Act, which prohibits unauthorized access of computers under certain circumstances; the Federal Records Act, which regulates the disposal of federal records; the Right to Financial Privacy Act, which prohibits access to financial records of individuals by government authorities; the Telephone Consumer Protection Act of 1991, which regulates telemarketing practices; and the Electronic

---

126 See Trans Union, 81 F. 3d at 230 (stating that information used implicitly transformed Trans Union lists into consumer reports).

127 See id., at 230.

128 See id., at 229; see also Ippolito v. WNS, Inc., 864 F. 2d 440, 451 (7th Cir. 1998) (holding that definition of “consumer report” in § 1681(a) is limited to information used in connection with business transaction involving one of consumer purposes set out in statute, that is, eligibility for personal credit or insurance, employment purposes and licensing).

129 See Wigod, supra note 33, at 123 (PARA). For a comprehensive examination of the Fair Credit Reporting Act, see Captain Julie J. R. Huygen, After the Deal is Done: Debt Collection and Credit Reporting, 47 A. F. L. Rev. 89, JC (1999) (PARA).


Communications Privacy Act of 1986, which prohibits, among other things, the intentional interception of electronic communications and the intentional access of stored electronic communications. Each of those statutes, however, falls short in addressing the unique concerns of online commerce. In fact, most of the privacy statutes appeal to the privacy concerns of the past and as such, fail to provide adequate safeguards against the prevailing privacy threats in today's electronic marketplace.

In addition to the inapplicability of the federal privacy statutes, even where information is covered by legislation, there is no central administrative agency to monitor compliance. The numerous agencies responsible for monitoring certain privacy issues include the Federal Trade Commission, the Office of Consumer Affairs, the Office of Management and Budget, the Office of the Comptroller of the Currency, the Social Security Administration, the Department of Health and Human Services, the Internal Revenue Service, the Federal Reserve Board, and the National Telecommunications and Information Administration. But although there are several federal agencies that oversee certain privacy issues, the power of those

Not Just for Breakfast Anymore: Federal Legislation and the Fight to Free the Internet from Unsolicited Commercial E-mail, 5 B.U. SCI. & TECH. L. 10, para. 10 (1999) (stating that autodialer messages are invasions of privacy); Howard E. Berkenblit, Note, Can Those Telemarketing Machines Keep Calling Me? - The Telephone Consumer Protection Act of 1991 After Moser v. FCC, 36 B.C.L. REV. 85, 85 (1994) (explaining that it is unlawful to initiate any telephone calls to residential telephones by artificial or prerecorded voices under Act).


See Wigod, supra note 33, at 123-26 (discussing above statutes and other federal statutes addressing privacy issues); Susan E. Gindin, Lost and Found Cyberspace: Informational Privacy in the Age of the Internet, 34 SAN DIEGO L. REV. 1153, 1196 (Summer 1997) (stating same); see also Pippin, supra note 7, at 147 (discussing various governmental agencies that monitor compliance).

agencies is limited in that their authority relates to issue-specific concerns. Additionally, the various agencies do not coordinate their efforts making privacy protection even more problematic.

D. Common Law

Tort law is the traditional means of redressing violations of privacy interests. Although the common law torts are collectively known as the invasion of privacy, they are actually four separate and distinct such common law torts. Those torts are: (1) intrusion upon seclusion; (2) public disclosure of private facts; (3) false light; and (4) misappropriation of name or likeness for commercial purposes. But, as discussed briefly


138 Intrusion upon seclusion imposes liability on "one who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns." Restatement (Second) of Torts § 652(b) (1977). Under this theory, an invasion is not considered intrusive unless it would be highly offensive to the reasonable person. Id. at cmt. c. Moreover, if the information intruded upon was voluntarily disclosed to the public, the seclusion right hasn't been violated. Id. at cmt. d. For instance, in Dwyer v. American Express Co., 652 N.E.2d 1351, JC (Ill. App. 1995), the court held that American Express had not violated the tort of intrusion upon seclusion when American Express had collected and sold information from its cardholders determining that the intrusion was tacitly authorized because the cardholder "voluntarily and necessarily" gave the information to American Express by using the card. Id. at 1356. The tort most relevant to E-mail interception or access is the "unreasonable intrusion upon the seclusion of another" tort. Gantt, supra note 133, at 374.

139 Under the public disclosure of private facts tort, there must be public disclosure (the disclosure must be such that the private fact is "substantially certain to become of public knowledge") of private facts (those facts a reasonable person would find the disclosure of highly offensive). Restatement (Second) of Torts § 652(d) (1977). The Restatement provides numerous examples of the type of information protected from disclosure: income tax returns, sexual relations and "unpleasant or disgraceful or humiliating illnesses." Id. Liability under the disclosure branch of invasion of privacy can be produced if an electronic bulletin board organizes and encourages users to disseminate E-mail messages obtained without the consent of the sender and addressee. Henry H. Perritt, Jr., Tort Liability. The First Amendment, and Equal Access to Electronic Networks, 5 HARV. J. L. & TECH. 65, 109 (1992).

140 Under the false light tort, one who gives publicity to a matter concerning another that places the other before the public in a false light is subject to liability to the other for invasion of his privacy, if (a) the false light would be highly offensive to a reasonable person, and (b) the actor had knowledge of or acted in a reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed. Restatement (Second) of Torts § 652(e) (1977).

141 The misappropriation tort applies when someone's name or likeness is used
below, the privacy torts have limited applicability in the online commercial world.

The torts of intrusion upon seclusion and public disclosure of private facts are rejected as a solution to online privacy concerns because most of the personal information obtained online is provided voluntarily by the user. Furthermore, "plaintiffs repeatedly lose such cases upon a showing that the fact in question was already in the public domain where, for example, it was obtained from a public record or other source outside the plaintiff's control, or obtained from the plaintiff directly while in a public place."\(^4\) The tort of false light is inapt because it requires an element of falsity.\(^3\) Because an online consumer's primary concern with respect to online privacy is that too much information will be disclosed, not that the information that is disclosed is not truthful, this tort is a non-starter. The tort of misappropriation of name or likeness for commercial purposes also has limited applicability to commerce on the Internet.\(^4\)

Information gathered online is not used to sell products or to associate the profiled subject with a particular product to use in a testimonial manner, rather the information is used in the decision-making process about marketing products or services online. Such information, although "appropriated" online, is not the appropriation that has historically been the subject of the tort of appropriation. Finally, it must be recognized that the Internet is a unique public forum in which certain pieces of information may be considered "personal" without really being "private", such as a phone number or an e-mail address. This blurred line makes

without their consent. \textit{Restatement (Second) of Torts} § 652(c) (1977). First Amendment concerns limit the use of this tort only to situations where the subject is not a public figure. \textit{Id.}

\(^{142}\) \textit{Belgium, supra} note 5, at 23 (noting that certain privacy torts have "been crippled by First Amendment precedents holding that no tort liability may attach to the press for giving further publicity to facts obtained from public sources."). Although the torts of intrusion upon seclusion and public disclosure of private facts are unlikely to apply to the disclosure of arguably public information such as names, addresses and phone numbers, release of other information on a more personal nature such as transaction histories may arguably trigger these torts.

\(^{143}\) \textit{See Reformation (Second) of Torts} § 652(e) (1977).

\(^{144}\) \textit{See Prosser & Keeton, supra} note 133, at 854 ("The effect of the appropriation decisions is to recognize or create an exclusive right in the individual plaintiff to a species of trade name, his own, and a kind of trademark in his likeness.").
application of the privacy torts easier said than done. Whatever common law tort remedy may theoretically be available, however, it is widely believed that the states will not even attempt to regulate privacy on the Internet because of the obvious difficulties such regulation poses including regulating a medium with no jurisdical boundaries.\textsuperscript{145}

IV. SAFEGUARDING CITIZENS' RIGHTS WITH COMPREHENSIVE PRIVACY LEGISLATION AND THE CREATION OF AN INDEPENDENT PRIVACY COMMISSION

The failure of existing statutory and common law to provide sufficient protections against information abuse in online commercial transactions requires the enactment of a new federal statute that directly addresses such concerns.\textsuperscript{146} Crafting such a proper privacy protection statute will be a complex endeavor.\textsuperscript{147} Indeed, legal scholars, practitioners and legislatures have proposed a wide-range of solutions to the privacy issue.\textsuperscript{148} Such reform requires a keen awareness of not only the technology itself, but also potential uses of the technology. Congress can no longer continue to avoid the issue of privacy rights by shaping

\textsuperscript{145} Cynthia C. Cannady and Katrin M. Cusack, \textit{Privacy Statements On The Internet: A Summary Of Applicable Law And A Practical Guide}, in \textit{THIRD ANNUAL INTERNET LAW INSTITUTE}, at 733, 738 (PLI Pat., Copyrights, Trademarks, & Literacy Prop. Course Handbook Series No. G0-0051, 1999) ("[I]t is safe to assume that the states will not attempt to regulate privacy on the Internet because of the obvious difficulty of regulating interstate, and international conduct.").

\textsuperscript{146} JAMES M. ATKINSON, RIGHT TO PRIVACY IN THE AGE OF TELECOMMUNICATION, 2 (1990) (declaring that "detailed examination of some of the privacy invasion issues in the rapidly changing telecommunications technology will demonstrate that the right to privacy cannot continue to be defined by a capricious approach.").

\textsuperscript{147} The United States is not the only country struggling to develop legislation governing commerce over the Internet. The need for global solutions have prompted assorted international bodies such as the European Union, the Organization for Cooperation and Development and the United Nations to examine the best methods for the protection of privacy over the Internet. \textit{See} Berman and Mulligan, \textit{supra} note 42, at 556. The current European model guarantees a wide-range of rights to insure the privacy protection of its citizens. \textit{See} Reidenberg, \textit{supra} note 58, at 776. The European system is premised on the theory of "self-determination" that "imposes responsibilities on data processors in connection with the acquisition, storage, use, and disclosure of personal information and, at the same time, accords citizens the right to consent to the processing of their personal information and the right to access stored personal data and have errors corrected." \textit{Id}.

\textsuperscript{148} \textit{See} Topping, \textit{supra} note 37, at 189 ("What is clear, however, is that legal scholars, practitioners, and legislators wield quite a number of different—and often conflicting—solutions to the perplexities of the Internet.").
“the right to privacy according to the public’s reactions to changes in the society.” 149 Congress must be proactive and promulgate legislation that will sufficiently regulate privacy in the context of the rapidly changing technology environment. 150

The legislation must provide clear guidelines to protect those who engage in online commercial transactions. It should regulate the collection, use and dissemination of all personal financial information regardless of whether the information is to be stored or sold to a third party. Congress should pass legislation that puts consumers back in charge of their personal information by mandating that before a commercial web site can collect any personally identifiable data, the consumer must expressly agree, or “opt-in” to such data collection. Then, if the consumer expressly agrees to allow his personal information to be collected, the commercial web sites must notify the consumer of exactly what information is being collected and how it will be used. The legislation must also provide some redress for consumers that are concerned about inaccurate information. Additionally, unlike existing legislation, the new statute must provide severe penalties for commercial Internet sites that violate the statute. 151

To establish a legal framework that provides predictable and uniform rules to regulate the collection and use of personal


150 See Mirzaian, supra note 145, at 136 (asserting that Congress can regulate electronic commerce pursuant to its commerce clause power); Stuckey, supra note 145, at 56 (suggesting that developments in electronic commerce require quick changes in law); John P. Tomaszewski, The Pandora’s Box of Cyberspace: State Regulation of Digital Signatures and the Dormant Commerce Clause, 33 Gonz. L. Rev. 417, 423 (1997) (stating that electronic commerce is interstate activity that will not be regulated by burdensome state statutes); see also U.S. Const. art. I, § 8, cl. 3 (granting Congress authority through Commerce Clause to regulate commerce among states and with foreign nations including ability to resolve most every issue that would arise under the rubric of electronic commerce).

151 Thus far, the simplest and least controversial legislative proposal for protecting privacy in online commerce is the Online Privacy Provision contained in Title III of the Internet Growth and Development Act of 1999, HR 1685. That proposal would require commercial web site operators that collect personally identifiable information to post a privacy policy and then to treat a violation of the policy as an unfair or deceptive trade practice. Id. This would, at a minimum, provide a baseline of privacy protection.
information, Congress must delegate some of its supervisory authority to an entity that can more readily ensure that existing laws and policies are continually examined and modified to adapt to new technology. Over the last few years, much has been made about the role of the FTC as the protector of privacy rights of Internet users.152 In fact, the FTC has held itself out as the de facto privacy agency in the United States and the regulatory agency primarily responsible for enforcing industry self-regulatory policies.153 But the FTC has fallen woefully short in its mandate and has produced minimal assistance in enforcing privacy rights for online consumers.154 Critics contend that the FTC has failed because it lacks the necessary expertise to develop and implement privacy policy.155

To effectively protect citizen privacy in electronic commerce, Congress should create an independent privacy commission to develop privacy legislation and lead the efforts to advance it both in the public and private sector.156 This independent privacy


153 See L. Richard Fischer, Privacy And Accuracy Of Personal Information, 3 N.C. BANKING INST. 23 (1999) (stating that FTC has conducted several workshops focusing on online privacy issues); Pippin, supra note 7, at 134 ("In short, the Commission [FTC] should generally be viewed as the primary agency responsible for consumer protection on the Internet and, specifically, for protecting Internet consumer privacy."); Melugin, supra note 79, at A18 (stating that FTC has "expanded their grip on the Internet").

154 See Belgum, supra note 5, at 136 (criticizing limited nature of FTC's proposed Internet-related privacy legislation); Angela J. Campbell, Self-Regulation and the Media, 51 FED. COMM. L.J. 711, 712-13 (1999) (stating that FTC's theme of electronic media self-regulation had not protected consumer privacy); Pippin, supra note 7, at 135 ("Despite the Commission's leadership role, its conclusions and especially its recommendations on addressing on-line privacy concerns have met with mixed reviews and dissent from consumer privacy organizations, Congress, and from within the Commission itself.").

155 See Reidenberg, supra note 58, at 791 (stating that existing governmental agencies are sectoral and lack expertise in cross-sectoral issues); see also Budnitz, supra note 54, at 867 (discussing consumer and privacy groups' criticisms of FTC); Pippin, supra note 7, at 134 (suggesting that FTC lacks authority to require businesses to adopt information practice policies); Saier, supra note 9, at 88 (stating that current and proposed federal protections of informational privacy are unsatisfactory).

156 See David Banisar, Roadblocks On The Information Superhighway, 41 FED. B. NEWS & J. 495, 495 (Aug. 1994) ("The United States is one of a few democracies without an independent, autonomous commission to examine the privacy implications of government actions."); Reidenberg, supra note 58, at 790 ("While counterintuitive for
commission would offer numerous benefits for both citizens and the online commerce industry.\textsuperscript{157} The commission would serve as a forum for collaboration with privacy experts, the public interest community, the government and the business community. Additionally, the commission would monitor developments in information technology and document their impact on personal privacy; develop public privacy initiatives; advise Congress about protecting the privacy of online consumers in the face of evolving technology and provide an objective voice to ensure that a careful balance between the interests of the online commerce industry to collect and disseminate information and the public's right to privacy are achieved.\textsuperscript{158}

Another benefit that an independent privacy commission can provide is prospective guidance to both the consumer and the Internet retailer. The commission would be empowered with the authority to grant safe harbor protections for company practices. Similar to the no-action letters issued from the Securities and Exchange Commission, a company seeking approval of certain policies could seek a request for approval from the commission.\textsuperscript{159}
Such an approval from the commission would mean that the company’s practices satisfy the legal standards for protecting personal privacy. Over time, those safe harbor decisions would provide a coherent body of public guidance and would increase the public’s awareness of information collection practices. This would, in turn, foster greater public participation in the privacy debate and hopefully lead to the public’s acceptance of online commerce.

V. CONCLUSION

The emergence of electronic commerce in today’s society has had a dramatic effect on the methods in which information is gathered, used and perceived. Information is no longer a means to an end, it serves as an end in itself. But while technological innovations allowing for commerce on the Internet have greatly improved our lives, they have come at a great price—the loss of personal privacy. Although the law provides limited privacy rights in certain narrow contexts and with respect to limited types of information, there is universal recognition of the need to ensure that proper measures are implemented to guard against informational abuses in online commercial transactions.

Privacy rights, of course, are not absolute and must be balanced with other competing interests such as the interests of commercial web operators in obtaining information to better serve the consumer. To date, however, the balance has tipped decidedly in favor of the web operators since it is the web

Loss of Privacy, 4 J. TECH. L. & POL’Y 3, 80 (1999) (discussing possible approaches to resolving privacy problems on Internet).

See Reilly, supra note 20, at 4 (“Privacy has evolved from a small single-function business into a complex conglomerate.”).

See Fulton, supra note 54, at 69 (“[W]ith the ease and convenience of new technology comes new avenues for user exposure to personal, political and business sabotage, and economic loss.”).

See Trubow, supra note 9, at 832 (“It is certainly this writer’s opinion that a regulatory framework for the Internet is necessary if it is to become a truly useful and reliable communications channel for business, government, and society. The current state of anarchy on the Internet renders the system inadequate for widespread, serious use.”).

There are several reasons why privacy interests on the Internet must not be absolute, such as the need to investigate and prevent hackers; to prevent and investigate the use of the Internet to coordinate or plan crime; to verify the accuracy of time billed to customers; and to allow employers to prevent the dissemination of trade secrets. See Wigod, supra note 33, at 95.
operators themselves that are making the rules. Because the regulation of data collection is vital to society's acceptance of the Internet as a commercial medium, formulation and implementation of comprehensive privacy legislation must be made a congressional priority.

The legislation should empower consumers through consent provisions and foster accountability through severe penalties for its violation. To spearhead those efforts, Congress should establish an independent privacy agency with the necessary expertise and resources to achieve a mutually beneficial equilibrium of legislative policy that regulates only as far as necessary to restrict abuses of privacy while contemporarily enabling technological progress. But whatever model of information privacy protection is adopted, it must be dynamic and subject to continual review so that it may be adapted to advances in technology.164

Consumer privacy protection on the Internet is a problem that will not be easily solved. We are now at the beginning of a long and complex process. We will constantly have to make decisions about how important we believe our right to privacy to be and exactly what measures we are willing to take to protect that precious right. But we must embrace the empowerment provided by ever-advancing technology instead of fearing its impacts. Online commerce promises enormous rewards for both consumers and merchants if the obstacles to privacy protection can be conquered.165

164 See Laurence Tribe, The Constitution in Cyberspace: Law and Liberty Beyond the Electronic Frontier, Keynote Address at the First Conference on Computers, Freedom and Privacy (PAGE) (1991) (stating that core constitutional principles, such as privacy, must be "invariable[le] . . . despite accidents of technology.").

165 See Reilly, supra note 20, at 4 ("(P)rivacy should be viewed as a foundational concept in the same manner that life, liberty, and the pursuit of happiness are foundational concepts in our society.").