1998

Privacy Online

Nick Allard
Brooklyn Law School, nick.allard@brooklaw.edu

Privacy On-Line: Washington Report†

by
NICHOLAS W. ALLARD*

† An earlier version of this article was presented at the *Hastings Communications and Entertainment Law Journal*'s Tenth Annual Computer Law Symposium, "The New Gold Rush: Defining the Digital Frontier," University of California, Hastings College of the Law, San Francisco, California, Jan. 31, 1998.

* Partner, Latham & Watkins, Washington, D.C.; J.D. Yale University, 1979; B.A. Oxford University, 1976; A.B. Princeton University, 1974. Mr. Allard is a member of the *Hastings Communications and Entertainment Law Journal* Advisory Committee and is a frequent contributor to the journal.

Introduction

Believe me when I say that it is really good to be here with you today. After spending the last ten days in the entertainment capital of the world—Washington, D.C.—it is just wonderful to escape from the vortex of swirling scandalous allegations, salacious rumors, and colorful characters and to get back to a normal, grounded, uneventful, mainstream kind of place like San Francisco. It is especially good to be here at Hastings once again, participating in its Tenth Annual Computer Law Symposium. Throughout the day the program will be examining important questions about how law is evolving for global computer networks. I am looking forward to hearing the impressive group of speakers who have been assembled by the COMM/ENT staff to tackle some of the toughest, most intellectually challenging, most timely legal questions posed by the explosion of electronic commerce in the United States and around the world.

I am no stranger to Hastings. This is the third time that I am kicking off the Computer Law Symposium, and I believe that so far I have had four articles published in COMM/ENT. You probably can blame one of your most illustrious graduates, Rachelle Chong, until recently a member of the Federal Communications Commission and still a good friend, who asked me to get involved with COMM/ENT several years ago. Even before that, when I clerked just down the street with Chief United States District Judge Robert Peckham, who unfortunately died a few years ago, well before his time, I had a close working relationship with Hastings students. Judge Peckham always made very good use of Hastings "externs." You know, those law students engaged in the terrific program that permits Hastings students to work for academic credit as part-time law clerks during the school term. So I have had many positive experiences, and a very healthy and sincere appreciation for the quality of Hastings students, for the quality of teaching here, and for this fine institution.

A few minutes ago, you heard Editor in Chief Matthew Passmore explain the title of today's program: "The New Gold Rush." I feel somewhat responsible for nudging this topic along and I must admit that I hope this particular topic generates more interest and better results than some of my previous efforts to steer the symposium in a particular direction. For example, a few years back I launched a somewhat tongue-in-cheek campaign to get Congress to enact a statutory prohibition on the overuse and abuse of annoying phrases such as "Information Superhighway," "National Information Infrastructure," and all the other inbred metaphorical progeny of this

species.[1] Later today you will hear professor Clay Calvert's much more serious and intriguing presentation about the impact of such metaphors.[2] I was just so sick and tired of hearing that, for example, the FCC Chairman was the "top cop" on the "infobahn," or hearing references about on-ramps, off-ramps, roadblocks, electronic traffic jams, tollbooths and such, that I hoped to find a replacement for the mother-of-all modern metaphors, the "information superhighway." So right here, from this podium, just a few years ago, I challenged the COMM/ENT staff to run a "Name the Thing" contest and to announce the results at the next computer law symposium.[3] Sadly, I can report that finding a better substitute proved to be quite difficult, and my efforts to send the phrase "Information Superhighway" into rhetorical retirement failed.

Then last year I gave a talk here and eventually published an article entitled *Law and Order in Cyberspace*,[4] (that particular symposium presentation has been expanded to a fourteen week course I am currently teaching at George Mason University School of Law). Last year's talk, and the new George Mason law school course, address the central question: "What is the appropriate role of government in regulating commercial activity conducted over electronic networks?" Other key questions examined were and are: "What should be the legal rules applicable to this electronic environment?" and "How will and should legal rules for cyberspace evolve?" To examine these questions we can, among other things, look to history to see how, as a matter of jurisprudence, law and order emerged and evolved in settings like, for example, the California Gold Rush era frontier that initially lacked a formal legal system. You see, it may not be completely accidental that today we're talking about "The New Gold Rush."

The New Gold Rush is indeed compelling policy makers, legislators, judges and prosecutors to deal with an explosion of legal issues presented by advanced communications and information technology. Although conducting business or interacting with people using 19th and 20th century lines of communication is governed by an

1. *See* Nicholas W. Allard, *Reinventing Competition*, 17 HASTINGS COMM/ENT L.J. 473, 480 (1995).

2. *See* Clay Calvert, *Regulating Cyberspace: Metaphor, Rhetoric, Reality, and the Framing of Legal Options*, 20 HASTINGS COMM/ENT L.J. 541 (1998).

3. *See* Nicholas W. Allard, *Commentary: Copyright from Stone Age Caves to the Celestial Jukebox*, 17 HASTINGS COMM/ENT L.J. 867, 868-69 (1995).

4. Nicholas W. Allard & David A. Kass, *Law and Order in Cyberspace: Washington Report*, 19 HASTINGS COMM/ENT L.J. 563 (1997).

array of criminal and civil laws, it is not so clear what rules do or ought to apply in the parallel world of cyberspace. As I noted here last year,[5] the relatively legally unfettered frontier of cyberspace often resembles gold rush era wild west boomtowns:

> populated with earnest PC pioneers and homestead users, Internet preachers, copyright rustlers, perverts, scam artists, and plain old crooks. There also will be some ghost towns if any of the early goldmines go bust, or if entrepreneurial prospectors continue to lose their shirts on attempts to make anything other than e-mail and entertainment pan out. And as in the old west territories, the first outpost of law and order is the federal judge, whose episodic justice sometimes encourages the bad guys because it reminds them of the infrequency of hangings.[6]

Talk about beating a metaphor to death.

I
Policy Context

Over the last year there have been significant developments marking the emergence of a framework for national and international cyberpolicy. These include the Clinton Administration's White Paper released in the Summer of 1997 which outlines its strategy for fostering business and consumer confidence in global electronic commerce.[7] Similar policy pronouncements were issued by a number of other countries.[8] Nevertheless, implementation of stated policies remains problematic. While the amount of Internet legislation introduced in Congress and in state legislatures has increased dramatically,[9] much of it is at odds with the Administration's policy

5. *See id.*

6. *Id.* at 567. The wild west metaphor is fairly popular. *See, e.g.*, Gary L. Bostwick, *Issue Spotting in Cyberspace*, COMM. LAW. 3, 5-6 (Winter 1998) (citing Rex S. Heinke & Lincoln D. Bandlow, *Roadblocks and Exit Ramps on the Information Superhighway*, PLI Handbook Litigating Libel & Privacy Suits, 203 (1996)). Some note that lawyers are settling cyberspace faster than the '49ers arrived in California. *See, e.g.*, Amy Harmon, *The Law Where There Is No Land*, N.Y. TIMES, Mar. 15, 1998, at D1.

7. President William J. Clinton, Vice President Albert Gore, Jr., A Framework for Global Electronic Commerce, Washington, D.C., July, 1997, (visited Mar. 23, 1998) <http://www.iiff.gov.eleccomm/exec_sum.htm> [hereinafter White Paper].

8. *See, e.g.*, European Commission, *Toward An Information Society Approach*, Green Paper on the Convergence of the Telecommunications, Media and Information Technology Sectors, and the Implications for Regulation (Brussels, Dec. 3, 1997) (on file with author).

9. The number of bills directly related to the Internet introduced in the 105th Congress at the time of this writing (91) is nearly double the number (50) introduced in the 104th Congress. Perhaps one of the most telling indicators of the widespread interest in Congress in the Internet is that the oldest member of the United States Senate, Strom Thurmond (R-S.C.), recently became the 100th member of the bicameral Congressional

framework and very few bills have been enacted. Consequently, many serious issues are unresolved. As controversies continue to arise, any federal legal vacuum will be filled in on a piecemeal basis by ad hoc judicial decisions, initiatives by state attorneys general and other state and local regulators, and by restrictions imposed on the United States from abroad. However, before turning to policy debates relating to various privacy issues, it may serve to offer three observations.

First, the federal government, and Congress in particular, are still far behind the curve in balancing the competing, legitimate interests that are at stake in developing the new rules needed for cyberspace.[10]

Second, when the federal government and Congress eventually get around to addressing issues of cyberlaw, lawmakers skip over the threshold issue of whether or not to fashion new legal approaches that best fit the reality of new technology for the 21st century. Instead, they proceed immediately to debate ways to tinker with and patch existing law originally developed for earlier technology.[11]

My third observation might seem at odds with the first two points: Although lawmakers are lagging behind on issues raised by new technology, there is time and ample reason to do the job of writing new rules well, whether the legal change be comprehensive and new, or merely a revision of existing legal rules.

It is worth noting, as we recently marked the fifty-second birthday of ENIAC, the first electronic computer, and as we marvel at the advanced state of computer technology in which an inexpensive, common pocket calculator has more brains that that first ENIAC, that today we are only somewhere in the "middle ages" of computer

---

Internet Caucus.

10. The hugely important so-called Year 2000 Problem or "Millennium Bug" also may not be receiving the attention it deserves from lawmakers or the public.

11. For example, the recommendations of the government's Internet Copyright Task Force Report eventually resulted in legislation introduced to amend our existing copyright law and thereby stretch the existing law to cover cyberspace—a law based on "Statute of Anne" principles originally applied to Gutenberg-era publishing technology. *See* Bruce A. Lehman, *Intellectual Property and Information Infrastructure Task Force Report of the Working Group on Intellectual Property Rights* (Department of Commerce, National Information Infrastructure Task Force Report) (1995); H.R. 2441, 104th Cong. (1995) (introduced by Rep. Carlos Moorhead (R-Cal.)). Another example is the tendency to apply existing communications regulatory models for broadcasting and common carriers to Internet issues, or to apply a hybrid model to such issues. See discussion of this phenomenon in Kevin Werbach, FCC Office of Plans and Policy, *Digital Tornado: The Internet and Telecommunications Policy* 26, 81 (1997) (on file with author). The Court's analysis in the recent successful challenge of the Communications Decency Act centered on whether First Amendment principles for common carriers or those for broadcasters applied. *See* Reno v. ACLU, 929 F. Supp. 824 (E.D. Pa. 1996), *aff'd*, 117 S. Ct. 2329 (1997); Shea v. Reno, 930 F. Supp. 916 (E.D.N.Y. 1996).

technology.[12] Updating laws for cyberspace might be somewhat behind schedule, but the dust has hardly settled on the latest innovations, and there are decades more of computer improvements and new uses for technology. So while lawmakers are at it, it is worth developing rules that are flexible, and will fit technology as well tomorrow as they might today.

Moreover, while technology is developing at a staggering pace, the human perspectives associated with the technology often remain the same through the years, centuries, and millennia. The policy fights and consensus-building that lie ahead over the uses of new technology, especially those that center on moral choices and values, are the same as those society has often encountered in the past. The Internet "has become a new battleground for refighting wars that shape our culture: society's attitudes toward sex and obscenity, libel, search and seizure, patent and copyright law, gambling, personal privacy and more."[13] And, as *Washington Post* columnist Meg Greenfield said:

> [m]y seemingly quaint, flapper-age parents, once they got the hand of the gadgetry, would be as at home in this world as we all would be in the super-duper one about to come. So far as its human inhabitants are concerned, we would have seen it all before.[14]

If one looks to history, it might, in fact, seem that humanity's uneasiness with information technology and society's search for the right response to communication innovations raise questions that are eternal. For example, the invention of writing, perhaps more so than the advent of the Internet in the modern world, created many concerns for ancient society.[15] The first references to writing, found in Homer's eighth century B.C. epic, *The Iliad*, demonstrate strong misgivings, and distrust of the manipulation of this information technology by government officials. The marks made by the illiterate Greek warriors in order to cast their lots for the usually fatal

12. *See* Andrea Stone, *We Are in the Middle Ages of Computers*, USA TODAY, Feb. 14, 1996, at 1A.

13. John Schwartz, *Deja Vu.com: The Internet Brings the Biggest Issues to the Fore Again*, WASH. POST, Feb. 15, 1997, at A1.

14. Meg Greenfield, *Back to the Future*, WASH. POST, Jan. 20, 1997, at A27.

15. I am indebted to S. Georgia Nugent, Professor of Classics at Princeton University, for her many insights into the similarities between information technology in Ancient Greece and our current policy debates on the subject. Recently Professor Nugent addressed this subject during a talk: *If Socrates Had E-mail...* (Mar. 1, 1997, Washington, D.C.) (paper delivered as part of symposium honoring 250th anniversary of Princeton University: *The Transformation of Learning in the Age of Technology*) (on file with author). Professor Nugent notes that even communication by speech was somewhat worrisome in classical antiquity for the archaic poets Semonides and Hesiod, the dramatist Euripides, and the historian Thucydides, who were all uneasy about the ability of women to speak. *Id.*

assignment to fight the Trojan hero, Hector, are what Homer called *semata lugra*, or "sorrowful signs."[16] Elsewhere in *The Iliad*, the hero Bellerophon is given a tablet containing "murderous symbols" that he must carry to a distant king.[17] The treacherous coded message in this, and many other narratives, such as the double, double-cross of Rosencrantz and Guildenstern in *Hamlet*, is "kill the bearer of this message." The presumption underlying these earliest references to writing in Western literature, that this innovation will be used to nefarious ends by unscrupulous men in power, will be familiar to anyone following the recent "clipper chip" and "encryption" debates in Washington, D.C. [18]

Similarly in the fifth century B.C., when Greek merchants began importing Egyptian paper into Athens, Socrates, one of history's great cranks, purportedly condemned the new technology. He was concerned, among other things, that it would disrupt the human ties that formed between philosopher and student, cause the mind and memory to atrophy, depersonalize interactions, and replace public discourse with less desirable and potentially dangerous private communication. Sound familiar? Compare Socrates' views to concerns many people have today about e-mail and cybersurfing and groups chatting over the Internet instead of over backyard fences. Later, Socrates' friend and protégé, Plato, attributed to Greek drama all of the criticisms that are today leveled against television; too violent, too much sex, too little educational content, and so on.[19] Athens could have used Jack Valenti to develop a ratings system.

Some 2,000 years later, when Gutenberg developed the movable-type printing press, many envisioned a communications revolution—specifically, that the printing press would put knowledge into the hands of the common man. For centuries, however the benefits of Gutenberg's invention were available mainly to the rich, academics

16. *Id.* at 3. HOMER, THE ILIAD OF HOMER, Bk. VII, at 172-72 (Richard Lattimore trans., Univ. of Chic. Press 1951). None of the warriors, who were illiterate, recognized, or at least acknowledged, that the lot that was drawn was indeed their own. It was "announced" that the lot bore Ajax's mark—who, it turned out, was the right choice, the warrior who ultimately defeated Hector.

17. HOMER, *supra* note 16, Bk. VI, at 165-75.

18. Nugent, *supra* note 15. The writing referred to in *The Iliad* is in effect coded, because the illiterate warriors and Bellerophon were unable to decipher it, but their leaders could read the coded language.

19. Carol Rigolot, Assistant Director, Program in Humanistic Studies, Princeton University, recently discussed this point, originally made by Alexander Nehamas, Director, Program in Hellenic Studies, Princeton University, in informal remarks at a meeting of Princeton alumni, Mar. 20, 1997, Washington, D.C.

and clerics. It was not until several hundred years later when the advent of public libraries and improved printing technology made books more affordable and widely available to the public. This history reminds us of the current policy debate over expanded universal service and appropriate ways to eliminate gaps between technology haves and have-nots. It suggests at least one great opportunity America has to improve upon the past by finding ways to put the benefits of technology into the hands of the public.

My students at George Mason dug up additional historical precedents for cyber-issues we face today, and I would be grateful to anyone else who would be good enough to add to the collection. For example, one student asserts that the historical development of literacy in revolutionary France was spurred by the mass appeal of increasing access to cheap pornography.[20] He suggests also that government and church efforts to restrict the free flow of this prurient material was a significant factor in organizing and fueling mass opposition that eventually toppled the French monarchy. He draws obvious comparisons with the current efforts to restrict cyberporn, and makes a much subtler observation about the many older people who are today learning how to use computers in order to gamble on-line—that their motives are comparable in some ways to those that made the French mob want to read.

Perhaps fortunately, the massively overhyped and still uncertain economic, social, and political ramifications of the Internet will not be felt fully for some time, giving lawmakers time to build a consensus and find solutions to both the age-old and novel legal and policy issues.

II
Privacy On-Line: Overview of the Problem

Perhaps the hottest, most intense policy debates in the United States and abroad on Internet-related issues center on escalating concerns over on-line security and privacy. National surveys conducted by Lou Harris and Associates report that eighty-five percent of Americans are concerned about their personal privacy, and that this is the single biggest reason keeping people from using the

20. I am obliged to Gerald Stegmaier, George Mason University Law School class of 1999 for this insight. His reference is ROGER CHARTIER, THE CULTURAL ORIGINS OF THE FRENCH REVOLUTION 38-91 (1991). *See also* Peter Johnson, *Pornography Drives Technology: Why* Not *to Censor the Internet*, 49 FED. COMM. L.J. 217 (1996).

Internet.[21] Hardly a day goes by when the morning papers do not contain a report or alarmed commentary about the erosion of privacy rights, usually purportedly caused by information technology. In the news are story after story about workers who are disciplined or discharged because of their employer learning about their on-line activity or because their employers obtain personal information about the employee on-line.[22] There are other stories about the disclosure of one's medical records,[23] driving records,[24] social security data,[25] and tax returns;[26] or about marketers, scam artists and criminals using information collected on-line to target individuals;[27] about intrusions

21. *See* ROBERT E. LITAN & WILLIAM A. NISKANEN, GOING DIGITAL (1998) (citing Alan Westin, *Data Protection in the Global Society,* Conference Report, American Institute for Contemporary German Studies (Berlin, Nov. 15, 1996)). *See also* LOUIS HARRIS & ALAN F. WESTIN, COMMERCE COMMUNICATIONS AND PRIVACY ON LINE, A NATIONAL SURVEY OF COMPUTER USERS (1997). The most recent polling data demonstrates that privacy concerns remain the primary reason why people do not use on-line services. *See Business Week/Harris Poll: Online Insecurity*, BUS. WK., Mar. 16, 1998, at 98.

22. One of the most publicized cases concerned the U.S. Navy's attempt to discharge a sailor, Chief Petty Officer Timothy R. McVeigh, which has been blocked by a federal judge, on the basis of information Navy investigators obtained from an anonymous on-line computer profile and confidential records held by an on-line service. Bradley Graham, *Judge Tells Navy Not to Dismiss Sailor With 'Gay' On-line Identity*, WASH. POST, Jan. 30, 1998, at A2; Philip Shenon, *Navy Case Combines Gay Rights and On-line Privacy*, N.Y. TIMES, Jan. 17, 1998, at A5.

23. In the Washington Metropolitan area, Giant and CVS pharmacies were reported to sell prescription data to a company that tracks people who do not refill prescriptions. In some cases the data company mailed sales pitches from drug companies to patients with certain illnesses. Giant and CVS have discontinued this practice. *See Privacy Issues in Daily Life*, WASH. POST, Mar. 8, 1998, at A18; Robert O'Harrow, Jr., *Prescription Sales, Privacy Concerns,* WASH. POST, Feb. 15, 1998, at A1.

24. Rajiv Chandrasekaran, *Eye at the Keyhole, Privacy in the Digital Age, Governments Find Information Pays*, WASH. POST, Mar. 9, 1998, at A1, A12 (discussing state government sales of information from driving records to data collection firms, and a new Maryland law that permits people to restrict access to their driving records).

25. In 1997 when the Social Security Administration announced that it would make people's benefit records available on-line, it was quickly forced to withdraw the program because the system was not sufficiently secure. Currently, a more limited service is available to individuals who clear several security checkpoints. It is also possible to request via e-mail that full information be sent by mail. *See* John Schwartz & Barbara J. Saffir, *Privacy Concerns Short Circuit Social Security's On-line Service*, WASH. POST, Apr. 10, 1997, at A23; *Blank Screen at Social Security*, WASH. POST, Apr. 11, 1997, at A26; M.J. Zuckerman, *Social Security Learned Tough Lesson in Privacy on the Web*, USA TODAY, Sept 4, 1997, at 4A.

26. Large numbers of IRS employees have been dismissed or otherwise sanctioned for electronically browsing through tax returns of celebrities, friends, neighbors, and family members. *See* Stephen Barr, *IRS Audit Reveals More Tax Browsing*, WASH. POST, Apr. 9, 1997, at A1.

27. *See* LITAN & NISKANEN, *supra* note 21, at 24-25; Elizabeth Corcoran, *Facing the Problems of Prank Messages, Bogus E-mail a Growing Issue on the Net,* WASH. POST, Mar.

from unwanted solicitations, telemarketing,[28] and stalkers;[29] and about data errors that cause serious problems for people.[30] Somewhere in this maelstrom of stories we can discern that, at least in America, when we talk about privacy we mean many, many different kinds of things, including confidentiality, anonymity, and avoidance of intrusion—the so-called "right to be let alone."

Public concern about various on-line privacy issues—which has been mounting for some time—has reached "critical mass," fueling intense, ongoing debates in the media, throughout industries involved in electronic commerce, in the executive branch, and in Congress. These debates include, for example, how to protect credit cards and other financial information on-line, how to protect people from abusive use of data collected by public agencies and private research groups, and what to do about advertisers pursuing children and World Wide Web sites secretly gathering and processing personal data about children.

Despite the increasing volume of public debate about privacy on-line, Internet users often do not realize that information about medical records, cellular phone calls, Internet usage, social security numbers, mothers' maiden names, and bank account numbers are susceptible to hackers, Internet providers, and the public at large. Although people are becoming much more sophisticated, novice computer users often mistake the apparent anonymity of e-mail and other modes of electronic communication for a blanket of privacy surrounding their personal data and on-line activities. Ironically, just the opposite is true. E-mail is, in fact, very public and can be visible to many network participants before it reaches its intended destination.

21, 1998, at D1.

28. Marcia Pledger, *Patients Worry About Privacy; Customers Complain About Telemarketing*, CLEV. PLAIN DEALER, Feb. 21, 1998, at A1; David Segal, *FTC Sues Online Marketer Over Spam Scam*, WASH. POST, Mar. 5, 1998, at E2; John Schwartz & Robert O'Harrow, Jr., *Databases Start To Fuel Consumer Fire*, WASH. POST, Mar. 10, 1998, at A1. A related problem which perhaps has not received as much attention is that of unwanted and intrusive government searches. *See* Michael Adler, Note, *Cyberspace, General Searches, and Digital Contraband: The Fourth Amendment and the Net-Wide Search*, 105 YALE L.J. 1093 (1996).

29. Colleen O'Connor & Laurie Wilson, *Women Battle Online Stalking*, DALLAS MORNING NEWS, Oct. 12, 1996, at 1A; Mark Grossman, *What To Do When On-line Stalker Strikes*, BROWER DAILY BUS. REV., May 9, 1997, at B1; Sheila Stainback, *Web Site Offers Methods of Finding Personal Information About People, Steals & Deals* (CNBC television broadcast, Sept. 29, 1997) (reporting about "Stalkers Home Page"); Virginia McCord, *Computer Opens Author's Home to Stalker*, WASH. POST, Feb. 19, 1998, at A2; Jeff Porter, *Online Stalkers*, ARK. DEMOCRAT-GAZETTE, Mar. 2, 1998, at D1.

30. *See* Chandrasekaran, *supra* note 24; Edmund Sanders, *Credit Reports Misrouted On-line*, ORANGE COUNTY REG., Aug. 16, 1997, at C1; LITAN & NISKANEN, *supra* note 21.

A party intent on "spying" on electronic transmissions can exploit the shortcomings of computer security, and gain access to private communications and data without leaving any trace or indication that the privacy of the communication has been compromised.[31]

This reality raises a myriad of issues. For example:

1. Should companies be able to profit by selling personal information? Or more generally, what private sector use may be made of personal information?
2. Should a company be able to use a person's billing information for non-billing purposes?
3. Should marketers be able to use information obtained from a "list service" to sell goods to potential customers?
4. To what extent do persons who "surf the net" consent to an invasion of privacy?
5. Junk e-mails or "spam"—should users have to tolerate bombardment by unsolicited e-mail advertisers?
6. Collecting information without a user's knowledge, most notably with "cookies" placed remotely on a user's own computer when they visit a website—should services be allowed to keep track of where users have been by recording their "mouse droppings?"
7. Should the general public have access to other people's personal information?
8. What protection should there be against the dissemination of social security numbers? Medical records? Addresses and telephone numbers? Spending histories? Credit card information? Bank account numbers?

Before attempting to address such issues, and in order to evaluate policy options and proposed solutions that governments around the world are considering, I believe that it is useful to take a step back and think about several threshold questions.

First, let's ask ourselves to think about and to distinguish between, on one hand, the erosion of privacy rights that is actually caused by new information technology; and on the other hand, the extent to which our perception that privacy is increasingly threatened actually reflects broader societal trends that are independent of

31. These are points made in an unpublished paper by Michael Wardell, *Should the Inmates Run the Asylum: Using Custom to Protect the Privacy of E-Mail and the Internet*, Law and Economics of Privacy Seminar, George Mason University School of Law (Apr. 2, 1997) (on file with author).

technological advances, or perhaps independent trends which are magnified by technological innovation.

William Safire of the *New York Times* recently railed about how privacy rights are being stripped away.[32] Let's look at his examples:

> Encouraged by an act of Congress, Texas and California now demand thumbprints of applicants for drivers' licenses—treating all drivers as potential criminals.
>
> Using a phony excuse about airplane security, airlines now demand identification like those licenses to make sure passengers don't exchange tickets to beat the company's rate-cutting promotions.
>
> In the much-applauded pursuit of "deadbeat dads," the Feds now demand that all employers inform the government of every new hire, thereby building a data base of who is working for whom that would be the envy of the KGB.
>
> Although it makes it easier to zip through tollbooths at bridges and highways, electric eyes reading license plates help snoopers everywhere follow the movements of each driver and passenger.
>
> Hooked on easy borrowing, consumers turn to plastic for their purchases, making records and sending electronic signals to telemarketers who track them down at home.
>
> Stimulated by this demographic zeroing-in, Internet predators monitor your browsing, detect your interests, measure your purchases and even observe your expressed ideas.
>
> And Big Brothers are not limited to government and commerce. Your friends and neighbors, the Nosy Parkers, secretly tape regular calls you make to them, and listen in to cellular calls to third parties, enhancing the video surveillance of public streets by government and private driveways by security agencies.[33]

"Enough!" Safire says, and calls for the end of the "creeping confluence of government snooping, commercial tracking, and cultural tolerance of eavesdropping."[34] What is particularly interesting to me is that none of the examples he cites are caused by technology, nor do the several solutions he proposes rely on technological fixes.[35] It is simply true that for whatever reasons, whether due to fear of crimes or terrorism, widespread use of credit cards, passivity, or inattention, Americans collectively are making more and more information about themselves available to others as we move through both the big events such as marriage, divorce litigation, bankruptcy, and even the

32. William Safire, *Nobody's Business*, N.Y. TIMES, Jan. 8, 1998, at A27.

33. *Id.*

34. *Id.*

35. Safire urges his readers to: (1) sign as little as possible; (2) support legislation that would require a "Privacy Impact Statement" before enacting any law; (3) use snail mail instead of e-mail; (4) persuade a Foundation to issue a quarterly "Intrusion Index"; and (5) pay cash. *Id.*

mundane routines of daily life in a modern world. We voluntarily give out personal data at banks, grocery stores, pharmacies and retail stores everywhere. (Why does a sporting goods store need to know my zip code when I buy a pair of running shoes?) We do it when we check e-mail or visit websites, apply for credit cards, use frequent flyer miles, use a cellular phone, and drive a car through an electronic traffic monitor or camera checkpoint that records whether traffic signals are observed.[36]

Indeed, some of the most publicized cases of invasions of privacy in recent memory had little to do with problems arising from the inherent nature of computer networks. The McVeigh case involved, among other things, a breakdown or nonobservance of statutory law, (the 1986 Electronic Communications Privacy Act), military rules ("don't ask/don't tell"), and internal company rules of the on-line service provider, all of which would have prevented disclosure of personal and arguably misleading information about McVeigh.[37] Reports about IRS employees snooping through the files of celebrities, neighbors, and others involved the improper and unauthorized use of computer files, but could have occurred, whether or not the private information was stored electronically.[38] In other words, it was a matter of employee misconduct and lack of effective supervision and control that was responsible, independent of the means used to breach private records. Even the much publicized shortcomings of the Social Security Administration's aborted web site that would have given taxpayers access to their social security records, involved the problem of inadequate means of authentication for those acquiring access to the records and not any problem fundamentally caused by computerized databases going on-line.[39]

Unquestionably the new technology, to a degree never before imaginable, enables and enhances the ability to gather, access, store, compile, search for and sort personal data.[40] Esther Dyson explains this development as well as anyone in her high energy, somewhat scatological, and very idiosyncratic new book, *Release 2.0*:

36. An excellent survey of such examples can be found in an extremely informative 3-part series, Robert O'Harrow, Jr., *Eye at the Keyhole: Privacy in the Digital Age*, WASH. POST, Mar. 8, 9, 10, 1998, at A1. See in particular Robert O'Harrow, Jr., *Eye at the Keyhole: Privacy in the Digital Age*, WASH. POST, Mar. 8, 1998, at A1, A18.

37. *See* Graham, *supra* note 22.

38. *See* Barr, *supra* note 26.

39. *See* Walter R. Houser, *SSA Balances Service, Citizen Privacy*, GOV'T COMP. NEWS, Nov. 10, 1997, at 23.

40. *See generally* O'Harrow, *supra* note 36, Mar. 8, at A1, A18; Federal Trade Commission, *Individual Reference Services, A Report to Congress* (Dec. 1997).

> The growing presence of the Web increases the ease of both collecting such data and assembling it. The interconnectedness of the net makes safeguarding privacy an increasing challenge: people are rightly concerned about the *combination* of data from different sources: web behavior, buying habits, travel history, income data. Often, facts are innocuous until combined with other facts.
>
> The user wants a seamless experience as he explores the Web, but he wants to appear as a discrete entity to each place he visits, with a legitimate identity revealed as appropriate—a credit rating, an employment record, a bank account, or a medical history. Indeed, a person's identity gets splashed all over the net in little fragments—no problem. But then someone in particular, anyone from a benign marketer only after a customer's business, to an employer, a stalker, or a blackmailer, can start collecting those fragments. One version of the problem is when the data are incorrect (and the user is the last to know); another version is when they are true.[41]

Of course, in addition to information voluntarily supplied by individuals on-line, there are other means of collecting personal information without a person's knowledge or consent, such as "cookies."[42] Dyson also vividly explains the extent that it is possible to track and monitor a web user's activities:

> Websites can keep track of what a person looks at, how long he stays, which ads provide the best response, whom he communicates with, what he says (in public discussion groups), how his behavior changes over the course of a day. Do drinkers buy more stuff in the evening, when they've had a few? Are customers of web catalogs more price-sensitive than customers of paper catalogs? Are people who book airline seats through the web more likely to be no shows? Are customers getting so sophisticated that middle seats will have to be priced lower to sell? Alternatively, would you be willing to pay extra for an aisle seat . . .?
>
> In principle, a merchant could compare a person's musical tastes to her reading preferences, or the political websites she visits to the magazines she reads. It could scour the newspapers and send e-mail to all people whose comments appeared in a particular site or matched a particular profile . . . .
>
> Some of this information is just statistical, but a lot of it marketers want in order to track you individually . . . . They [also] want to track your behavior. The problem is that the information they gather has a way of spreading . . . .[43]

Obviously, those concerned about coping with new threats to privacy need to take account of trends that both are and are not driven by technology.

---

41. ESTHER DYSON, RELEASE 2.0 196 (1997) (emphasis in original).
42. *See id.* at 197.
43. *Id.* at 199.

Another large question that is central to the current policy debate on privacy issues is, to the extent that advanced information technology undermines privacy, can its impact on individual privacy be controlled? Can you protect privacy with technology, with market-based approaches involving self-help and self-regulation, or with legal rules enforced by government or a combination of these solutions? Some like Dyson favor a combination of technology and free market self-help.[44] One of the assumptions underlying the concept that on-line business will effectively safeguard privacy is that privacy is a service that will "sell." Consumers will either pay for privacy or opt not to. Others, and you will hear more about this later today during Dierdre Mulligan's presentation, are concerned that markets are imperfect and consequently we cannot rely completely on market-based self regulation.[45] There is, it is argued, a compelling need for the government to be involved in regulating the information that, for example, on-line companies gather about consumers who lack a realistic choice of vendors, or children, and to provide a meaningful opportunity to learn about and correct errors.[46]

A third threshold issue is whether new laws need to be enacted to apply to the Internet setting. This question is actually quite complex. Just as in America there is no single concept of privacy, there is no overarching law or set of principles in this country that deal with the privacy of personal information much less a single government entity responsible for protecting privacy. There are excellent surveys of the crazy quilt of constitutional precedents recognizing implied privacy rights (there is no explicit mention of privacy in the Constitution), and federal and state laws which apply to privacy on-line which I can commend to you.[47] While it has been more than a century since Justice Brandeis described privacy as "the right to be let alone"[48] and

44. *See id.* at 201.

45. *See* Dierdre Mulligan, *Classifying Electronic Privacy*, presentation at the Tenth Annual Computer Law Symposium, "The New Gold Rush: Defining the Digital Frontier," (Jan. 31, 1998) (videotape on file with the *Hastings Communications and Entertainment Law Journal*). *See also* LITAN & NISKANEN, *supra* note 21, at 62.

46. *See* LITAN & NISKANEN, *supra* note 21, at 62.

47. *See, e.g.*, JONATHAN ROSENOER, CYBERLAW, THE LAW OF THE INTERNET 129-60 (1997); ON-LINE LAW, THE SPA'S LEGAL GUIDE TO DOING BUSINESS ON THE INTERNET 269-78 (Thomas J. Smedinghoff, ed., 1997). *See also* EDWARD A. CAVAZOS & GAVINO MORIN, CYBERSPACE AND THE LAW, YOUR RIGHTS AND DUTIES IN THE ON-LINE WORLD 13-31 (1995); EXECUTIVE OFFICE OF THE PRESIDENT, OFFICE OF MANAGEMENT AND BUDGET, OPTIONS PAPER ON PRIVACY (1997).

48. *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890); RESTATEMENT (SECOND) OF TORTS § 652A, Comment a. *See also* Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J. dissenting), *overruled by*

the Court has also discerned several privacy rights in different parts of the Constitution, there are no rulings directly and definitively applicable to many of the on-line privacy issues of increasing concern to the public. Paradoxically, while there are numerous federal and state statutes that apply to aspects of electronic communication and information technology, statutes, for example, dealing with interception and disclosure of electronic communications,[49] protection for government-maintained data bases,[50] regulation of credit reports[51] and financial records,[52] telemarketing,[53] and the so-called "Bork law" that protects video rental records,[54] to mention just a few, many experts conclude that there are few effective safeguards that protect personal data on-line, that there are gaping holes in the coverage of existing laws, and many existing provisions are inconsistent if not contradictory.[55]

Do we need privacy laws that just apply to the on-line environment or should privacy rights be protected more universally? Do we need a more comprehensive approach or should lawmakers continue to focus and attempt to fix more specific issues? Do we in the United States have the ability to act unilaterally in pursuing legal change when the reality of electronic computer networks is that they are global? These are just a few of the not so small issues lawmakers face as they attempt to fashion solutions for problems affecting privacy on-line.

Katz v. United States, 389 U.S. 347 (1967).

49. Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2701 (1986).

50. Privacy Act of 1974, 5 U.S.C. §§ 552a-559 (1994).

51. Fair Credit Reporting Act of 1970, 15 U.S.C. §§ 1681-1681t (1994).

52. Right to Financial Privacy Act, 12 U.S.C. §§ 3401-3422 (1995).

53. Telephone Consumer Protection Act of 1991, 47 U.S.C. § 227(b)(1) (1991).

54. Video Privacy Protection Act of 1988, Pub. L. No. 100-618, 102 Stat. 3195 (1988) was enacted to protect information about movie videos people buy or rent after such information was disclosed during the confirmation process of Supreme Court nominee Robert Bork.

55. *See* LITAN & NISKANEN, *supra* note 21, at 24-26, 60-65; Robert O'Harrow, Jr., *Laws on Use of Personal Data Form a Quilt With Many Holes*, WASH. POST, Mar. 9, 1998, at A12.

III
Status Report on Federal Privacy Initiatives: Search for Solutions

A. Summary

Privacy, or more specifically, the lack of it in an on-line world, is also one of the biggest new issues before federal agencies and on Capitol Hill. Although numerous security (i.e., encryption) and privacy bills were introduced in the 105th Congress, some of which became the subject of hearings, Congress has been unable to reach agreement on any of the on-line privacy issues. The bills receiving the most attention include those dealing with encryption policies, computer security, the cloning of cellular phones, and interception of cellular phone calls. Other bills designed to restrict on-line disclosure of Social Security numbers and other personal identification and to curtail the practices of Internet junk e-mails, have seen no action. Industry efforts to address privacy issues, steps taken by data collection companies to self-regulate, and the Federal Trade Commission's recent decision to give this approach a trial, probably will hold off further legislative action in this Congress—with the possible exception of a breakthrough compromise on encryption bills and perhaps privacy bills designed to protect children from on-line advertisers.

B. Administration Policy Statements

In 1995 the Privacy Working Group of the United States Information Infrastructure Task Force ("IITF") issued a report entitled "Privacy and the National Information Infrastructure—Principles for Providing and Using Personal Information."[56] The report recommends that certain principles should govern the collection, processing, storage, and re-use of personal data. The foundation of these principles are the concepts of "awareness" and "choice." The report concludes that:

- Data-gatherers should inform consumers what information they are collecting, and how they intend to use such data; and
- Data-gatherers should provide consumers with a meaningful way to limit use and re-use of personal information; and

56. PRIVACY WORKING GROUP OF THE UNITED STATES INFORMATION INFRASTRUCTURE TASK FORCE, PRIVACY AND THE NATIONAL INFORMATION INFRASTRUCTURE—PRINCIPLES FOR PROVIDING AND USING PERSONAL INFORMATION (1995).

- Consumers are entitled to redress if they are harmed by improper use or disclosure of personal information or if harmed by inaccurate, outdated, incomplete, or irrelevant personal information.[57]

With public concern about on-line privacy continuing to grow and possibly constraining the development of electronic commerce, the Information Policy Committee of the IITF prepared a draft paper on "Options for Promoting Privacy on the National Information Infrastructure," and initiated further study of the subject.[58] Other federal agencies recently have also been studying privacy issues. The National Telecommunications and Information Administration issued a report titled "Privacy and the NII: Safeguarding Telecommunication-Related Personal Information"[59] which examines the IITF Privacy Principles as applied to "telecommunications" and advocates a voluntary framework of rules based on "notice" and "consent." In early 1997 the Federal Trade Commission issued first a staff report focusing on the direct marketing and advertising industries[60] and then followed up with extensive public hearings on consumer privacy.[61] These various policy studies and papers culminated in the privacy sections of the Administration's White Paper on regulating global electronic commerce, the so-called "Magaziner Report," released in July, 1997 by the White House.[62] In sum, the Clinton Administration supports private sector efforts already underway to implement self-regulatory privacy regimes, including mechanisms for facilitating awareness and the exercise of choice on-line, and for evaluating how well private industry implements fair information practices.[63] I note here that there is a useful description and analysis of such mechanisms in Esther Dyson's new book,[64] and Robert Litan and William Niskanen's new book.[65]

57. *Id.*

58. INFORMATION POLICY COMMITTEE OF THE IITF, OPTIONS FOR PROMOTING PRIVACY ON THE NATIONAL INFORMATION INFRASTRUCTURE (Apr. 1997).

59. NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION, PRIVACY AND THE NII: SAFEGUARDING TELECOMMUNICATION-RELATED PERSONAL INFORMATION (Oct. 1995).

60. STAFF REPORTS, FTC PUBLIC WORKSHOP ON CONSUMER PRIVACY ON THE GLOBAL INFORMATION INFRASTRUCTURE (Jan. 7, 1997) [hereinafter FTC REPORT].

61. FTC PUBLIC WORKSHOP ON CONSUMER INFORMATION PRIVACY (June 1997).

62. White Paper, *supra* note 7, at 11-14.

63. *Id.*

64. *See* DYSON, *supra* note 41, at 202-10 (chapter entitled "Privacy" discussing a disclosure and validation system called TRUSTe and the "Platform for Privacy Preferences" which is designed to give users more control over their personal information).

65. *See* LITAN & NISKANEN, *supra* note 21, at 60-61, (discussing TRUSTe and the

While optimistic that technology and self regulation could provide solutions to privacy concerns, the Administration recognizes that if privacy concerns are not adequately addressed by industry through self-regulation and technology, there will be increasing pressure for government to play a more direct role in safeguarding consumer choice regarding privacy on-line. Moreover, particular concerns are expressed about the use of information gathered from children, who may lack the cognitive ability to recognize and appreciate privacy concerns: The White Paper states "parents should be able to choose whether or not personally identifiable information is collected from or about their children."[66] Accordingly, the Administration urged industry, consumer, and child-advocacy groups working together to use a mix of technology, self-regulation, and education to provide solutions to the particular dangers arising in this area and to facilitate parental choice.[67]

C. FTC Approval of Self-Regulation

On December 17, 1997, the FTC released a report that analyzes and generally approves several guidelines developed by industry that are designed to limit the availability of certain types of personal information.[68] The Commission's study analyzed computerized databases—services that disseminate personal identifiable information, often referred to as "individual reference services" or "look-up services"—which are used to locate, identify, or verify the identity of individuals. The report summarizes how these services work, examines their risks and benefits, and details the self-regulatory principles proposed by a consortium of such services that will, among other things, prohibit distribution to the general public of Social Security numbers, mother's maiden names, and birthdates, if obtained

---

Open Profiling Standards which enables users to specify what information they wish to reveal on websites and to disable "cookies").

66. White Paper, *supra* note 7, at 13.

67. *Id. See also Statement of the Federal Trade Comm. on 'Internet Privacy,' Hearings Before the Subcomm. on Courts and Intellectual Property of the House Judiciary Comm.* text accompanying notes 28-35 (testimony of David Medine, Mar. 26, 1998) (visited Mar. 31, 1998) <http://www.house.gov/judiciary/41178.htm> [hereinafter Medine Statement]. The FTC staff found that 80 of 100 commercial websites surveyed were collecting personal information from children, without seeking parental permission. *Id.* at text following note 37.

68. Federal Trade Commission, *Individual Reference Services, A Report to Congress*, (Dec. 1997). This report was requested by Senators John McCain (R-Ariz.), Ernest Hollings (D-S.C.), Richard Bryan (D-Nev.) and former Senator Larry Pressler (R-S.D.). For the FTC's most recent report on Internet privacy, see Medine Statement, *supra* note 67.

from *non*-public sources. Important issues regarding consumers' access to public information obtained or compiled by the look-up services remain to be addressed. The FTC expressed concern, for example, that individuals have no way of discovering or correcting errors that may have occurred in the transcription, transmission, or compilation of this information. The guidelines also do not provide any limitations on the availability or uses of public records and publicly available information. Accordingly, they do not limit the potential harm that could stem from access to and exploitation of sensitive information in public records and publicly available information. In addition, they do not provide individuals with a means of accessing public records and other publicly available information maintained about them by individual reference services.

A great deal of information about consumers is available through individual reference services. This often sensitive personal identifying information comes from a variety of public and non-public sources. According to the Commission's Report, the industry guidelines developed by the Individual Reference Services Group ("IRSG") address most concerns raised by the dissemination of non-public personal identifying information.[69] They:

> impose restrictions on access to certain 'non-public information.' The restrictions vary according to the category of customer. In general, customers that have less restricted access to non-public information are subject to greater controls. Conversely, the general public has more restricted access to non-public information including social security numbers, maiden names, and birthdates.[70]

According to the voluntary industry principles agreed to by the signatories:

> Individual reference services will not distribute to the general public certain non-public information, such as Social Security number, mother's maiden name, birth date, credit history, financial history, medical records, or similar information, or any information about children.
>
> They also will not make available unlisted telephone numbers obtained from sources other than public records, or unlisted addresses obtained from the telephone company.
>
> Look-up services may not allow the general public to run searches using a Social Security number as a search term.

69. The IRSG consortium includes the following companies: Axiom Corporation; CDB Infotek, a ChoicePoint Company; DDS Information Systems; Database Technologies, Inc.; Equinox Credit Information Services, Inc.; Explain; First Data Solutions, Inc.; Information America, Inc.; IRS, Inc.; LEXIS-NEXIS; Metromail Corporation; National Fraud Center; Online Professional Electronic Network; Trans Union Corporation. *See id.*

70. FTC REPORT, *supra* note 60, at Executive Summary.

> Consumers will be allowed to obtain access to the non-public information maintained about them and to opt-out of the non-public information distributed to the general public.
>
> Look up services may not make available information gathered from marketing transaction[s].[71]

The look-up services must maintain facilities and systems that will prohibit unauthorized access to non-public information and create an "audit trail." They also must undergo an annual compliance review by an independent third-party to verify that the guidelines have been followed, the results of which will be made public. In addition to this very important monitoring requirement, companies purchasing information from IRSG members must be contractually bound to comply and to also undergo audits.

According to the IRSG, its guidelines should reach ninety percent of personal data collected on-line by the time they bring their practices into compliance by the end of 1998.[72] The FTC's decision is consistent with the Administration's "Global Framework" White Paper and has been formally endorsed by the White House.[73] It is less clear, however, whether the FTC's decision to allow self-regulation, even though backed by independent audits and possible FTC intervention, is consistent with the tough privacy directive that goes into effect later this year in Europe.[74]

D. Developments Abroad

As the European Union Directive demonstrates, the United States is hardly alone in tackling privacy issues. Privacy concerns are being raised in many countries around the world. Some countries have enacted laws, implemented industry self-regulation, or instituted administrative solutions designed to safeguard their citizens' privacy.

---

71. FTC Release, *Information Industry Voluntarily Agrees to Stronger Protections for Consumers, FTC Says*, Dec. 17, 1997, at 3 (visited Mar. 23, 1998) <http://www.ftc.gov/opa/9712/inrefser.htm>.

72. *See FTC Backs Industry Plan for Self-Regulation on Dissemination of Sensitive Personal Data, Electronic Information Policy & Law Report* (BNA), Dec. 24, 1997, at 1332-33 [hereinafter *Electronic Information Policy & Law Report*]. IRSG members have agreed to revisit the problem of how to deal with inaccurate personal data and to quantify the extent of online inaccuracies by June 1999. *See* Medine Statement, *supra* note 67, at text accompanying note 20.

73. *Electronic Information Policy & Law Report, supra* note 72.

74. *See* European Union Policy Directive (Directive 95/46/EC) (effective Oct. 1998) discussed in Peter Q. Swire & Robert Litan, *Avoiding a Showdown Over EU Privacy Laws*, BROOKINGS POLICY BRIEF NO. 29 (Feb. 1998) and their forthcoming book, PETER Q. SWIRE & ROBERT LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE AND THE EUROPEAN PRIVACY DIRECTIVES (forthcoming 1998).

While privacy is a serious matter everywhere, different countries have very different approaches.[75] Disparate policies could emerge that might disrupt transborder data flows. A prime example, as I have suggested, is the European Union which in October 1995 adopted a directive that prohibits the transfer of personal data to countries, that, in its view, do not extend adequate privacy protection to EU citizens.[76] Initial reactions of European officials as to whether the FTC approach would pass muster were not favorable; however, recently observers are more optimistic about the prospects for an accommodation.[77]

To ensure that differing privacy policies around the world do not impede the flow of data on the Internet, the Clinton Administration indicates it will engage its key trading partners in discussion to build support for industry-developed solutions to privacy problems and for market driven mechanisms to assure customer satisfaction about how private data is handled.[78] Specifically, it will continue policy discussions with the EU nations and the European Commission to increase understanding about the American approach to privacy and to assure that the criteria they use for evaluating adequacy are sufficiently flexible to accommodate our approach. The United States also will enter into a dialogue with trading partners on these issues through the Asia Pacific Economic Cooperation ("APEC") forum, the Summit of the Americas, the North American Free Trade Agreement ("NAFTA"), and the Inter-American Telecommunications Commission ("CITEL") of the Organization of American States. These discussions are led by the Department of Commerce, through NTIA, and the State Department, and include the Executive Office of the President, the Treasury Department, the FTC and other relevant federal agencies. NTIA is also working with the private sector to assess the impact that the implementation of the EU Directive could have on the United States.

E. Proposed Federal Legislation

Congress and state legislatures are increasingly active in the privacy arena as well. By my count, in the present 105th Congress over 200 bills have been introduced that are related to privacy or encryption as compared with forty-five bills in the 104th Congress. At

75. *See European Union Policy Directive*, *supra* note 74, at 16.

76. *See id.* at 29.

77. *Electronic Information Policy & Law Report*, *supra* note 72; BROOKINGS POLICY BRIEF, *supra* note 74.

78. White Paper, *supra* note 7, at 13.

the state level, one count puts the number of privacy bills introduced in 1996 at more than 8,500.[79]

Congress will continue to be drawn into the task of striking a balance between the need for the free flow of information and the need to protect privacy, including the need to secure communication and stored information in the increasing on-line economy. Security and privacy on the Internet are clearly interrelated. In order for people to feel comfortable in the networked environment, their electronic information must be secure. Too little security and people will be reluctant to rely more on computer networks; however, too much security will also impede the flow of information. Law enforcement and national security authorities insist vigorously that in the information age they need more than ever to be able to monitor criminal and terrorist activities by electronic eavesdropping.[80] So far, the Clinton Administration, over the strong opposition of United States businesses and civil liberties groups, as well as many other countries,[81] has sought to prevent the use of security technologies it cannot pierce to obtain information said to be essential for law enforcement and national security purposes.

1. Encryption Legislation

One solution to computer security problems is to code or encrypt messages or data, disguising them as an unintelligible scramble of numbers and letters which can only be decoded or deciphered by those who have the keys or the algorithms that were used to scramble the message in the first place. The readable message is thus called the *plaintext*, the encrypted message the *ciphertext*. Litan and Niskanen explain it far more coherently than I ever could:

> The strength of the encryption, or how easy it is to crack, depends on the robustness of the algorithm used and/or the length of the string of characters used in the key, measured in bits. Currently, weak encryption uses forty-bit keys; stronger encryption uses fifty-six bit keys that are more than 65,000 times harder to attack [technology which the Administration has sought to prevent from being exported]. Most banks now use 128 bit or even stronger

79. *See* Robert O'Harrow Jr., *Eye on the Keyhole: Privacy in the Digital Age: Data Firms Getting Too Personal?*, WASH. POST, Mar. 8, 1998, at A1.

80. *See, e.g.*, John Markoff, *Clinton Continues to Stumble Over the "E" Word (Encryption)*, N.Y. TIMES, Feb. 27, 1998, at C1; Roberto Suro, *Reno Threatens Legal Battle to Ensure Electronic Surveillance*, WASH. POST, Feb. 27, 1998, at A13.

81. Recently, for example, the Organization for Economic Coordination and Development rejected the United States' proposal to permit the world's law enforcement authorities to eavesdrop on computer transmissions. *See* John Markoff, *U.S. Rebuffed in Global Proposal for Eavesdropping on the Internet*, N.Y. TIMES, Mar. 27, 1997, at A1.

> security . . . encryption techniques are used by governments around the world to protect military secrets, by private companies to protect confidential information, and by financial institutions as they exchange payment and other sensitive data.[82]

Encryption technology keeps improving and evolving, and several new techniques may ultimately provide a breakthrough to the four year old controversy that has surrounded this issue.[83]

In light of the need for encryption, and all of the problems accompanying it, lawmakers are faced with three basic choices when regulating encryption technology. First, they can do nothing. If the government did not regulate the sale and export of this technology, software manufacturers would sell whatever products they desired at home and abroad. Although U.S. consumers would have ready access to the latest encryption products, criminals and terrorists would similarly have free access to these products. This technology may give those criminals the ability to avoid government surveillance and detection, making it easier to use computer technology to facilitate money laundering, terrorism, and other crimes.

The second policy choice available to the government is to bar forms of encryption so powerful that the government cannot break them. As a preliminary matter, such an action by the government may not be constitutional. Even if this action were constitutional, however, the government would be forcing private parties to use weaker forms of encryption that could be broken easily by other private parties. Such a lack of security would compromise the utility of the Internet for business transactions and would very likely stunt the growth of electronic commerce and put American businesses at a disadvantage overseas.

The third option is a middle path between banning and deregulating strong encryption, and this appears to be the choice of the Clinton Administration. The Administration is allowing private parties to use and export strong encryption, as long as the government has access to the keys necessary to break the code.[84] While this option

82. GOING DIGITAL, *supra* note 21, at 22. *See also* ONLINE LAW, *supra* note 47, at 497-504.

83. *See* Markoff, *supra* note 80 (discussing new Hewlett Packard and Cisco Systems techniques). For a description of this controversy, including the U.S. statutes which govern the export of encryption, and recent regulatory changes and judicial decisions, see Allard & Kass, *supra* note 4, at 573.

84. Public key encryption is a system of encryption where every individual has two keys; one public key to encrypt messages, and a second, private key used to decrypt messages. This is in contrast to a system of private key encryption, where the same key is used to lock and unlock messages. In a system of public key encryption, strangers can send encrypted messages without agreeing beforehand on the key to unlock the messages. In a

does allow parties to use more advanced encryption products in their private communications, it raises a host of civil liberties concerns. These concerns have derailed the Administration's efforts to date, and several legislative proposals regarding encryption were considered in the 104th Congress, including bills that would deregulate encryption. While these bills died in Committee, many have been reintroduced in the 105th Congress.

In the House of Representatives there were five different versions of the Security and Freedom Through Encryption Act, H.R. 695,[85] that have been reported out of various committees. Three of those versions favor strong encryption and two favor a sort of watered-down encryption that would provide the government with a so-called key recovery system enabling the government to intercept and monitor transmissions. In the Senate, the situation at the time of this writing, is similarly confused. S. 909, the Secure Public Networks Act,[86] introduced and revised by Senator John McCain (R-Ariz.) and Senator Bob Kerrey (D-Neb.), has been the primary focus of debate. It reflects many of the positions advocated by law enforcement. Majority leader Trent Lott (R-Miss.), however, opposes S. 909 in its present form, which is a strong indication that it faces difficulties getting to the floor of the Senate for action by the full Senate. Meanwhile, at this writing, the Administration has been drafting its own encryption bill. Among other things, it is expected to make key management infrastructure voluntary, and to specify the conditions for releasing key recovery information to the government.

While there remains a great deal of disagreement about the issue, the debate has become much more focused in 1998. So while it is a fluid, volatile situation, encryption is an issue which could get resolved this year or in the next Congress. Now that may seem to you to be a really wimpy prediction, but it's not, really, when you consider the prospects for legislation relating to other on-line topics, such as copyright, for which I am not confident that we will see a legislative solution in this century, if ever. And in terms of "dog-years" and "Washington-years," saying "this year" or "next year" means a lot can

---

private key system, parties can send and read encrypted messages only if they already know the other parties' secret key. Because electronic commerce requires large-scale communications between strangers, a system of public key encryption is vital. *See* Don Clark, *Security Dynamics Unit and Cylink End Patent Row,* WALL ST. J., Jan. 7, 1997, at B6; Don Clark, *Bizdos is Holding the Key to Guard Internet Secrets,* ASIAN WALL ST. J., Apr. 17, 1996, at 12.

85. H.R. 695, 105th Cong. (1997).

86. S. 909, 105th Cong. (1998).

happen in that time. Ultimately, I believe that developments abroad, new options presented by technological innovations, and the reality that strong encryption is necessary will drive all the parties to compromise and hammer out a solution that can be enacted by Congress.

2. Privacy Legislation

In contrast to proposed encryption legislation, the prospects for Congressional action on various privacy bills, with some limited exceptions, is much more remote for the foreseeable future. The immediate impact on Congress of the FTC's decision to give industry (IRSG) self-regulation a chance to work, and the uncertainty over how this approach can be reconciled with the European Union's privacy rules, probably will derail any action on privacy legislation this year.

For example, there were four privacy bills that were referred to the House Telecommunications Subcommittee that have not yet seen any action at all. To give you a sense of their coverage: (1) H.R. 98, introduced by Representative Bruce Vento (D-Minn.), would prohibit interactive computer services from disclosing personal information about subscribers without consent;[87] (2) H.R. 1287, introduced by Representative Bob Franks (R-N.J.), would bar interactive computer services from disclosing a person's social security number or personally identifiable information derived from that number without a person's consent;[88] (3) H.R. 1964, introduced by Representative Ed Markey (D-Mass.), is a more comprehensive measure designed to protect consumers and children;[89] and (4) H.R. 2368, introduced by Subcommittee Chairman Billy Tauzin (R-La.), would create an industry working group to develop voluntary guidelines for self regulation,[90] a measure which probably helped propel, but is now moot by virtue of the recent IRSG and FTC proposals.

Similarly, the Personal Information Privacy Act, S. 600,[91] introduced by Senator Diane Feinstein (D-Cal.), which would prohibit the use of Social Security numbers without consent, is not making any progress. Despite significant concern about unwanted junk e-mail, no progress has been made on anti-spam legislation in either the House

87. H.R. 98, 105th Cong. (1997).
88. H.R. 1287, 105th Cong. (1998).
89. H.R. 1964, 105th Cong. (1998).
90. H.R. 2368, 105th Cong. (1998).
91. S. 600, 105th Cong. (1997).

or the Senate. The Netizens Protection Act, H.R. 1748,[92] introduced by Representative Chris Smith (R-N.J.), would outlaw sending unsolicited commercial e-mail advertisements. S. 875, introduced by Senator Robert Toricelli (D-N.J.), would require an on-line seller or service to observe requests by users to "opt out,"[93] has been referred to the Senate Commerce Committee, where it languishes.

H.R. 1367, the Federal Internet Privacy Protection Act,[94] introduced by Representative Thomas Barrett (D-Wis.) and Representative Sue Kelly (R-N.Y.), would allow people to sue the federal government for releasing confidential information. No hearings have been held on this bill.

There are, however, some areas where there could be privacy legislation, if not in this Congress, then in the next. First, children's privacy bills have some momentum, despite strong opposition from industry. For example, S. 771, introduced by Senator Frank Murkowski (R-Ark.), requires advertisers to label messages as advertisements and also requires Internet service providers to offer customers blocking software to filter out advertisements.[95] The premise underlying this measure is that children cannot discern as well as adults between program content and advertising, and do not know when they are the target of a sales pitch. (Having recently enjoyed watching the latest James Bond movie, *Tomorrow Never Dies*,[96] which weaves promotional material for rental cars, cellphones and many other products into the script, I must say I am sympathetic, but skeptical, that it is possible to draw a bright line between programming and ads in any medium). In the House, H.R. 1972, the Children's Privacy Protection and Parental Empowerment Act,[97] introduced by Representative Barney Franks (D-Mass.), would make it a crime to knowingly sell personal information about a child absent parental consent. This measure is pending before the House Crime Subcommittee.

Another bill worth noting is not directly related to the Internet, but instead focuses on prohibiting cloning and intercepting cellular telephone transmissions, and is expected to be enacted.[98] After a conference call involving a pivotal strategy session for Speaker

92. H.R. 1748, 105th Cong. (1998).
93. S. 875, 105th Cong. (1997).
94. H.R. 1367, 105th Cong. (1998).
95. S. 771, 105th Cong. (1997).
96. TOMORROW NEVER DIES (Paramount 1997).
97. H.R. 1972, 105th Cong. (1998).
98. H.R. 2369, 105th Cong. (1998).

Gingrich was overheard and tape recorded in late 1996, the Republican leadership started to push legislation that the House recently passed to crack down on cellular telephone privacy and eavesdropping, H.R. 2369.[99] A similar Senate bill, S. 493, the Wireless Telephone Protection Act,[100] was approved by the Senate in November 1997. The companion to S. 493, H.R. 2460, passed the House with amendments in February 1998.[101] Presumably there will be legislation enacted in this area this session. While Internet access with mobile, wireless units is increasingly a reality, and as such would be affected by the proposed legislation, perhaps the most compelling point to be made here is the power that a legislator's own personal experiences have to overcome legislative gridlock and move a measure through Congress.

Third, the Senate Commerce Committee favorably reported a bill, S. 1619, the Internet School Filtering Act,[102] sponsored by Chairman John McCain (R-Ariz.), which is designed to protect students from accessing pornography and other inappropriate material on-line in schools and libraries that their parents and school authorities wish to filter out and block. The bill would cut off new federal Internet subsidies for schools and libraries that do not install equipment to block indecent material. Most observers conclude that this measure is far less susceptible to a first amendment challenge than, for example, the Communications Decency Act ("CDA") which was overturned in *ACLU v. Reno*.[103] A revised version of the CDA, S. 1482, which Washington wags have dubbed "CDA-lite," has been introduced in the 105th Congress, but is given little prospect of enactment.[104]

IV
Conclusion

Progress by lawmakers in fashioning substantive rules for privacy on-line is slow but steady—and that is just fine. Many of the privacy issues seem familiar, and they are, because they are controversies that go back at least to the founding of this country, and are only now masquerading as novel information age questions, sometimes

99. *Id.*
100. S. 493, 105th Cong. (1997).
101. H.R. 2460, 105th Cong. (1998).
102. S. 1619, 105th Cong. (1998).
103. *See* Reno v. ACLU, 929 F. Supp. 824 (E.D. Pa. 1996), *aff'd*, 117 S. Ct. 2329 (1997).
104. *See* S. 1482, 105th Cong. (1998).

overdressed in techno-babble. Some of the threats to privacy seem acute, whether because an international showdown is looming over purportedly inconsistent national privacy laws, as could be the case with the United States and Europe, or because a threat to privacy touches a moral nerve or involves those individuals, such as children, who may need others to protect them. Neither familiarity nor contempt are good grounds to rush to adopt new legal rules, or to impose special new regulations, just for electronic networks. First, lawmakers, like doctors, should take care to do no harm. It should not be assumed that the heavy regulatory frameworks established over the last century for telecommunications, radio and television broadcasters, cable and satellite, and electric utilities were either optimal, or are now desirable to mimic and apply to electronic commerce over computer networks. Competition, empowering individuals to engage in self help through mechanisms of disclosure and enforceable informed consent, and using technology to provide solutions that strengthen personal privacy, can go a long way toward addressing today's and tomorrow's privacy concerns without stunting the growth of still infant on-line business and other electronic networked enterprises. Still, there is an important role for government. Among other things, government provides the necessary cop on the beat, to enforce rules, but not necessarily regulate behavior. In the once libertarian frontier of cyberspace, most legitimate business leaders now would concede that Dodge is a better place when Matt Dillon is in town. The government also plays an important role by stepping in when market and other private mechanisms fail to adequately protect the privacy of individuals. This is, for example, the whip hand the FTC holds over the IRSG industry, which indicates it will use its existing statutory authority to go after information collection and dissemination practices when the voluntary self-regulatory principles do not work. The other role for government is to work for international cooperation and accommodation of different rules arising in different countries and cultures, a function which is, after all, critical in light of the global nature of computer networks. This is the role the United States government will play, and probably play successfully, to avoid a trade crisis with the European Union over the implementation of the EU's Privacy Directive later this year.

In reality, the development of law and policy for privacy on-line is just starting, and society is only now beginning to address the more difficult aspects of the issue. In all likelihood, achieving intelligent,

workable balances among the competing interests in order to uphold privacy on-line is an effort for which there may be no end.