

# Internet Privacy: An Overview of Domestic and International Issues and Policy Responses

November 1999



# Table of Contents

<b>Introduction</b> . . . . .	1
<b>Pending Legislation</b> . . . . .	2
Online Privacy . . . . .	2
Financial Privacy . . . . .	4
Medical Privacy . . . . .	5
State Initiatives . . . . .	6
<b>The Federal Communications Commission</b> . . . . .	6
Customer Proprietary Network Information (CPNI) . . . . .	7
Communications Assistance for Law Enforcement Act (CALEA) . . . . .	7
Cable Protection of Subscriber Privacy . . . . .	8
<b>The Federal Trade Commission</b> . . . . .	9
Enforcement Actions . . . . .	11
<b>The Clinton Administration's Efforts</b> . . . . .	12
<b>Industry Self-Regulation</b> . . . . .	14
<b>International Round Up</b> . . . . .	17
<b>Conclusion</b> . . . . .	20

# Internet Privacy: An Overview of Domestic and International Issues and Policy Responses

November 1999

## Introduction

---

One of the most difficult tasks facing lawmakers and policymakers today is balancing the competing interests of consumers' privacy with businesses' opportunity in the new electronic economy. While the need to balance privacy against economic interests has always existed, the technological capabilities of the Internet have underscored the importance of safeguarding these critical interests and have threatened in new ways expectations about personal and commercial privacy. It is often stated that a key to the continued growth and use of the Internet and the expansion of e-commerce is consumer confidence and reasonable expectations regarding the use of personal information—in other words, the ability of consumers to feel assured that their personal information is not being impermissibly shared or sold. This report provides a snapshot of current Internet privacy issues and proposed solutions.

As an overview, the report addresses several broad areas. First, the report describes current federal legislative efforts to address various aspects of Internet-related privacy issues. As of this writing, there were numerous pieces of legislation under consideration in the House and Senate, all aiming to secure in some measure the privacy of Americans who use the Internet. As a general

matter, these privacy issues can be classified into three general categories: (1) general online privacy; (2) financial privacy; and (3) medical privacy.

Second, the report reviews the efforts of federal agencies to address Internet privacy issues. For example, the Federal Communications Commission (FCC), an independent agency, has addressed in some measure consumer expectations and rights with respect to the privacy of their communications and their network information. In addition, the Federal Trade Commission (FTC) has been extremely active, examining a broad range of issues, including those related the privacy of children. Similarly, the Clinton administration has been actively involved in monitoring and addressing privacy-related issues. Each recently issued rules to promote privacy protection and enforce current regulations.

Third, the report examines the efforts of industry to address these issues as participation by the industry is central to privacy protection. In this regard, the report reviews the efforts of online industries that have collaborated in a self-regulatory manner to ensure that consumers' privacy is respected on the Internet.

Finally, as the Internet provides seamless access to information and products across geographic borders, the report briefly examines the international efforts underway to provide seamless privacy protection across national borders.

To assist the reader, titles of important bills, government organizations and industry groups are identified in **bold**. Endnotes are included for general reference. As with any report addressing the Internet, we urge the reader to seek and obtain information that updates the information provided, as the area is, of course, a moving target.

## **Pending Legislation**

---

The area of privacy is far reaching and has far-reaching implications. As such, we have seen a flurry of legislation that addresses various aspects of privacy and the Internet. While the scope of the legislation is broad, it is useful to categorize these efforts into federal legislation that address online privacy, financial privacy, and medical privacy as well as other state legislative efforts.

### **Online Privacy**

As the use of the Internet has grown, the issue of online privacy—that is, the protection of consumers' personal information—has garnered increased attention, and has spurred numerous pieces of legislation.

For example, the **Networking and Information Technology Research and Development Act**<sup>1</sup> was approved on September 9, 1999 by the House Science Committee and authorizes an Internet privacy study. Rep. David

Wu (D-Ore) was responsible for the amendment to the bill that directs the National Science Foundation and the National Academy of Science's National Research Council to collaborate. The bill directs the two agencies to (1) recommend technologies that could be developed to improve privacy on the Internet; (2) analyze private and public programs that implement privacy standards, policies, and technologies; and (3) study international privacy protection plans.

Similarly, another important piece of legislation is the Online Privacy Protection Act of 1999.<sup>2</sup> This bill would require the FTC to prescribe regulations requiring websites and online services to post notices about the collection and use of personal information. Also, individuals would be given greater control over the collection of their information and the opportunity to "opt out" of having their personal information disclosed. Introduced in the Senate by Senator Burns (R-MT) on April 15, 1999, this bill was referred to the Senate Commerce Committee. Hearings were held on July 27, 1999.

Another piece of legislation, the **Electronic Rights for the 21<sup>st</sup> Century Act**,<sup>3</sup> has as its goal the implementation of uniform privacy standards and procedures for information on computer networks, information collected by Internet registrars, loan and library records, law enforcement access to location information, roving wiretaps, decryption assistance for encrypted communications and stored electronic information, and other purposes. This bill was introduced in the Senate by Senator Patrick Leahy (D-VT) on April 21, 1999, and referred to the Judiciary Committee.

Likewise, the **Consumer Internet Privacy Protection Act of 1999**<sup>4</sup> was to require consumer notification and written consent before disclosure of personal information to a third party. Individuals would be afforded a private cause of action and the right to learn what personal information is being maintained. Further, this bill confers enforcement and investigative authority upon the FTC. The bill was introduced in the House by Rep. Vento (D-MN) on January 6, 1999 and referred to the House Commerce Committee. On April 12, 1999, the bill was referred to the Subcommittee on Telecommunications, Trade, and Consumer Protection.

Of particular interest is the subject of privacy of minors. **The Children's Privacy Protection and Parental Empowerment Act of 1999**<sup>5</sup> is designed to protect children's privacy by imposing criminal liability for its violations. The bill imposes criminal liability on anyone selling information about children under the age of 16 without written parental consent. Moreover, this

---

<sup>1</sup> See H.R. 2086, 106<sup>th</sup> Cong. (1999).

<sup>2</sup> See S. 809, 106<sup>th</sup> Cong. (1999).

<sup>3</sup> See S. 854, 106<sup>th</sup> Cong. (1999).

<sup>4</sup> See H.R. 313, 106<sup>th</sup> Cong. (1999).

<sup>5</sup> See H.R. 369, 106<sup>th</sup> Cong. (1999).

bill affords parents the right to learn what information a list broker maintains, the right to stop further disclosure, and a private cause of action. The military, the National Center for Missing and Exploited Children, and colleges will remain exempt from the provisions of this bill. On January 19, 1999, Rep. Bob Franks (R-NJ) introduced this bill in the House where it was referred to the House Committee on the Judiciary. The bill was referred to the Subcommittee on Crime on February 25, 1999.

Finally, the **Social Security On-line Privacy Protection Act**<sup>6</sup> would require that an interactive computer service not disclose an individual's social security number, or personal information, which can only be obtained by means of the social security number, without prior written consent. The FTC will have enforcement authority. The bill was introduced in the House by Rep. Bob Franks (R-NJ) and on January 19, 1999 was referred to the House Commerce Committee. On January 29, 1999 the bill was referred to the Subcommittee on Telecommunications, Trade, and Consumer Protection.

### Financial Privacy

There are also several measures designed to protect financial information, often viewed as critical to the growth of electronic commerce. Congress passed groundbreaking legislation called the **Financial Services Modernization Act of 1999**<sup>7</sup> on November 4, 1999, which was signed into law on November 11, 1999<sup>8</sup>. The Act, which overhauls the financial services industry, permits banks, insurers, and securities firms to merge and sell everything from checking accounts to stocks, bonds, and life insurance.<sup>9</sup> The legislation contains some privacy protection giving consumers control over how banks and other companies use personal financial information, but more importantly, allows states to enact tougher privacy laws.<sup>10</sup> That late addition to the bill may simply shift this controversial issue to the states, as many state attorneys general are already examining the information gathering and marketing practices of banks.<sup>11</sup>

The Financial Information Privacy Act of 1999<sup>12</sup> would give the Security and Exchange Commission (SEC) the authority to issue rules to protect the privacy of confidential consumer information. This bill would require the SEC to implement regulations: requiring consumer consent before dis-

---

<sup>6</sup> See H.R. 367, 106<sup>th</sup> Cong. (1999).

<sup>7</sup> See S. 900, 106<sup>th</sup> Cong. (1999).

<sup>8</sup> See Robert O'Harrow Jr., *A Postscript on Privacy*, Washington Post, Nov. 5, 1999, at E1 and Marcy Gordon, *Clinton Signs Banking Overhaul Bill*, Associated Press, Nov. 11, 1999.

<sup>9</sup> See Kathleen Day, *Revised Bank Bill Clears Key Roadblock*, Washington Post, Nov. 3, 1999, at E1.

<sup>10</sup> O'Harrow, *supra* note 8.

<sup>11</sup> *Id.*

<sup>12</sup> See S. 187, 106<sup>th</sup> Cong. (1999).

closing information to a third party; affording consumers the right to review and access their confidential information; and precluding information sharing between financial institutions and their agents or affiliates. This bill was introduced in the Senate on January 19, 1999 by Sen. Paul Sarbanes (D-MD) and referred to the Banking, Housing, and Urban Affairs Committee. On June 9, 1999, the Committee on Banking, Housing, and Urban Affairs held hearings on the bill.

The Securities Investors Privacy Enhancement Act<sup>13</sup> mandates that brokers, dealers, investment companies, and advisors protect customer privacy and the confidentiality of their financial information. Section 2 of this bill would amend the Securities and Exchange Act of 1934 to require brokers to inform clients when information is being collected about them, including information collected by an affiliate or agent and obtain written consent before disclosing information. Section 3 of the bill would amend the Investment Company Act of 1940 to require investment companies to keep confidential the identities of a company's outstanding securities owners. Finally, Section 4 of the bill would amend the Investment Advisors Act of 1940 to require investment advisors to keep their clients personal information confidential. The bill was introduced in the House by Rep. Markey (D-MA), referred to the House Commerce Committee on March 25, 1999, and was referred to the Finance and Hazardous Materials Subcommittee on April 12, 1999.

The objective of the **Bank Secrecy Sunset Act**<sup>14</sup> is to amend the portions of the Bank Secrecy Act that require banks to perform mandatory financial record-keeping, monitor customer accounts, or obtain information concerning any person in connection with a financial transaction (including the source of funds involved in the transaction). This bill was introduced by Rep. Paul (R-TX) and referred to the House Committee on Banking and Financial Services on Feb. 3, 1999. The bill was later referred to the Subcommittee on Financial Institutions and Consumer Credit on February 25, 1999.

## Medical Privacy

The developments of both the Internet and electronic databases have increased the threats to medical records privacy. There is considerable fear that private medical information could be inappropriately used for example by a bank to deny credit or an employer to reject an employment application. As a result, there has been widespread support in Congress for legislation to protect individuals' privacy with respect to medical records.<sup>15</sup>

<sup>13</sup> See H.R. 1340, 106<sup>th</sup> Cong. (1999).

<sup>14</sup> See H.R. 518, 106<sup>th</sup> Cong. (1999).

<sup>15</sup> See *Summary of Medical Records Privacy Bills in the 106<sup>th</sup> Congress*, Tech Law Journal (visited July 29, 1999) <<http://www.techlawjournal.com/cong106/privacy/medical/Default.htm>>.

The purpose of the **Medical Information Privacy and Security Act (MIPSA)**<sup>16</sup> is to ensure personal privacy concerning health-care matters and afford individuals the right to access their personal health information. In addition, this bill retains the ability of a state to impose criminal and civil penalties for the unauthorized use of health care information. Sen. Leahy (D-VT) introduced this bill in the Senate and referred it to the Senate Labor Committee on March 10, 1999 where a hearing was held on April 27, 1999.

Likewise, the **Medical Information Protection Act (MIPA)**<sup>17</sup> seeks to ensure confidentiality with respect to medical records and health care-related information, and for other purposes. The bill was introduced in the Senate by Sen. Burns (R-UT) and referred to the Committee on Health, Education, Labor, and Pensions on April 26, 1999. The Senate Labor Committee held a hearing regarding medical record privacy on April 27, 1999.

### State Initiatives

In addition to federal legislation, it is also notable that several states have introduced privacy initiatives of their own. For example, California has introduced the Personal Information and Privacy Act of 1999 (S.B. 129) that calls for legislative findings and declarations regarding the right to privacy.<sup>18</sup> The Arizona House of Representatives has also passed a Bill (H. 2639) establishing a 12-member study committee to study the Internet, including such issues as Internet privacy, jurisdiction, regulation, and taxation.<sup>19</sup> Similarly, Connecticut has established the Office of Privacy Counsel within the Department of Information Technology to monitor state privacy issues.<sup>20</sup> As Internet usage increases, it is reasonable to expect state efforts to expand.

## The Federal Communications Commission

---

While consumer privacy is not generally an issue within the jurisdiction of the Federal Communications Commission, there are several areas in which it arises. Most notably, these include customer proprietary network information and the implementation of the **Communications Assistance for Law**

---

<sup>16</sup> See S. 573, 106<sup>th</sup> Cong. (1999).

<sup>17</sup> See S. 881, 106<sup>th</sup> Cong. (1999).

<sup>18</sup> See *State Bill Creating EU-Style Privacy Rights Amended, Leaving Hortatory Call for Findings*, 4 Electronic Commerce & Law Report, No. 15, at 321 (Apr. 14, 1999).

<sup>19</sup> See William Carlile, *Legislation Advances in Arizona House Authorizing Study Group on Internet Laws*, 4 Electronic Commerce & Law Report, No. 11, at 241 (Mar. 17, 1999).

<sup>20</sup> See Martha Kessler, *Connecticut Considers New 'Privacy Counsel' to Safeguard Privacy of Government Records*, 4 Electronic Commerce & Law Report, No. 16, at 339 (Apr. 21, 1999).

**Enforcement Act**, that addresses the ability of law enforcement to intercept digital communications.

### **Customer Proprietary Network Information (CPNI)**

The conflict between an individual's right to privacy and a corporation's right to free speech is highlighted in the approach the FCC has taken toward customer proprietary network information (CPNI). In its orders, the FCC has implemented the congressional directive to protect the confidentiality of consumer information and telephone records that relate to their usage of the network and services delivered through the network.<sup>21</sup> Significantly, once the FCC acted, US WEST, an incumbent local exchange carrier (ILEC) sued, claiming the FCC's rules violate carriers' free speech guarantees under the First Amendment by requiring carriers first to obtain customer permission for marketing purposes, the so-called "opt-in" approach. This summer, the U.S. Court of Appeals for the 10th Circuit agreed, overturning the FCC's decision and vacating the FCC's rules.<sup>22</sup> In its August 18, 1999 decision, the court held that the CPNI implementation rules under section 222 of the Communications Act were too restrictive and violated carriers' right to free commercial speech under the First Amendment.<sup>23</sup>

Notably, although the FCC adopted revised CPNI rules in its second order on Reconsideration just days before the 10<sup>th</sup> Circuit's decision, it is unclear if this order will ever be enforced. The court's decision essentially allows carriers to use their preferred "opt out" provision, putting the burden on customers to tell carriers not to use their information for marketing campaigns or to sell their information to telemarketers. The ILECs argue that this approach will decrease the number of telemarketer calls, as it allows a more targeted approach for the telemarketers, while others argue that it will increase the number of telemarketing calls.<sup>24</sup> The FCC asked the court for a rehearing either of the original three-judge panel or the full panel<sup>25</sup> and several consumer advocates have intervened in support of the FCC's request.<sup>26</sup>

### **Communications Assistance for Law Enforcement Act (CALEA)**

Since it has passed, CALEA has been the subject of a FCC implementation effort as it attempts to define the scope of the obligation imposed upon carri-

<sup>21</sup> See 47 U.S.C. § 222 (1996).

<sup>22</sup> See *US West, Inc. v FCC*, 182 F.3d 1224 (10<sup>th</sup> Cir. 1999).

<sup>23</sup> See *id.* at 1240.

<sup>24</sup> See Tom Woodruff, *Phone Companies Win and You Lose Your Privacy*, MSN Money Central (Nov. 1, 1999) <<http://moneycentral.msn.com/articles/news/capital/4774.asp>>.

<sup>25</sup> See *FCC to Appeal CPNI Case*, TR Daily, Aug. 25, 1999.

<sup>26</sup> See *Consumer, Privacy Groups, Scholars Urge Court To Reconsider CPNI Decision*, TR Daily, Oct. 26, 1999.

ers to ensure their networks are sufficiently accessible to law enforcement. Note that CALEA has no effect on law enforcement's ability to obtain a court order, such as a search warrant, to require an information service provider to turn over information about its subscribers or intercept their communications. Instead, it simply defines the scope of the obligation of telecommunications carriers to make technical changes to their networks to accommodate surveillance.

As a result of the FCC's implementation efforts, the Electronic Privacy Information Center (EPIC) and American Civil Liberties Union (ACLU) filed suit in the U.S. Court of Appeals for the District of Columbia Circuit challenging the FCC's August 1999 order implementing CALEA.<sup>27</sup> The parties claim that the ruling, which requires the telecommunications industry to design its systems to comply with FBI technical requirements to facilitate electronic surveillance, exceeds statutory requirements and violates federally protected privacy interests.<sup>28</sup>

### Cable Protection of Subscriber Privacy

Under Section 631 of the Cable Communications Policy Act of 1984, as amended,<sup>29</sup> cable operators are required to abide by specific requirements to protect subscribers of cable services or other services. The privacy restrictions of Section 631 generally concern the notification, collection, use, and disclosure of personally identifiable information by the cable operator regarding cable subscribers. The provision requires a written statement at least once annually regarding the nature of the information collected; the nature, frequency and purpose of any disclosure; the period the information will be maintained; and the time and place the subscriber may have access to the information. Disclosure of the information is strictly limited and requires prior written or electronic consent. Significantly, the provision applies not only to traditional cable services, but also to other services and thus implicates by its terms Internet access. As drafted, these provisions are limited in scope to apply to a "cable operator," as defined specifically in the section, rather than to a third-party user of the cable system that is unaffiliated with the cable operator. The term "cable operator" is defined to include, (a) "any person or group of persons who provides cable service over a cable system and... owns a significant interest in such cable system or who otherwise controls... such a cable system," and (b) any entity that is "owned or controlled by, under common ownership or control with a cable operator."

---

<sup>27</sup> *Groups Initiate Court Challenge To FBI Wiretap Standards; Say FCC Decision Threatens Communications Privacy*, <http://www.epic.org/privacy/wiretap/>, rel. Nov. 18, 1999.

<sup>28</sup> *Id.*

<sup>29</sup> 47 U.S.C. § 551.

## The Federal Trade Commission

---

In contrast to the FCC, the Federal Trade Commission has greater direct responsibility to address consumer privacy issues. In response to the growing attention to privacy issues, the FTC has been extremely active.

Over a year and half ago, on June 4, 1998, the FTC issued a report to Congress summarizing the then current state of online privacy collection endeavors, industry self-regulation, as well as various studies on the industry principles used in information collection, use, and dissemination.<sup>30</sup> The report concluded, “Industry’s efforts to encourage voluntary adoption of the most basic fair information practices have fallen short of what is needed to protect consumers.”<sup>31</sup> Further, a FTC survey revealed that almost 90% of websites collect personal information from consumers, including personal information from children. The FTC recommended that Congress develop legislation requiring notice and parental consent before websites collect any information from children.

Today, the FTC continues to encourage the widespread implementation of effective protections for consumers’ online privacy. To pursue this goal, on July 13, 1999 the FTC issued a report to Congress summarizing the current state of online privacy.<sup>32</sup> Notably, the report concluded that legislation to address online privacy is not appropriate at this time, emphasizing that self-regulation is the most effective and least intrusive means to ensure fair information practices on the Internet. The report also outlines the FTC’s agenda which includes two public workshops to address: (1) the ability of a website to track a consumer’s online activity and collect information; (2) the establishment of a task force to understand costs associated with implementing fair information practices; (3) the establishment of another task force to create incentives encouraging the development of privacy enhancing software; and (4) joint efforts with the Commerce Department to promote education on privacy for private sector businesses. This report was presented to the Senate Commerce Committee’s Communications Subcommittee on July 27, 1999.

In June of 1999, Mary J. Culnan, a professor at Georgetown’s McDonough School of Business, released a progress report to the FTC titled “**Georgetown Internet Privacy Policy Study (GIPPS)**.”<sup>33</sup> The purpose of this study was to provide the FTC with objective data regarding the status of online privacy for “consumer favorite” commercial websites. The study

<sup>30</sup> See *Privacy Online: A Report to Congress* (June 4, 1998) <<http://www.ftc.gov/reports/privacy3/index.htm>>.

<sup>31</sup> See *id.*

<sup>32</sup> See *Self-Regulation and Privacy Online: A Report to Congress*, Federal Trade Commission (July 13, 1999) <<http://www.ftc.gov/reports/privacy3/index.htm>>.

<sup>33</sup> See *Georgetown Internet Privacy Policy Study (GIPPS Report)* (June 8, 1999) <<http://www.msb.edu/faculty/culnanm/gippshome.html>>.

addressed the following questions: What personal information do websites collect from consumers? How many websites posted privacy disclosures? Do these disclosures reflect fair information practices? The study found that, of the 361 websites sampled, 92.8% of the sites in the sample collected at least one type of personal information, 65.9% posted at least one type of privacy disclosure, and 13.6% of the 236 websites that collected information contained at least one survey item for notice, access, security, and contact information. This study was included in the FTC's July 13, 1999 report to Congress.

In other actions, on April 20, 1999, the FTC issued a proposed **Children's Online Privacy Protection Rule**.<sup>34</sup> The proposed rule requires website operators to post a notice of how information collected about children under the age of 13 will be used. The proposed rule also establishes standards for parental consent and access requirements. Finally, the rule includes a safe harbor provision by which interested parties may seek FCC approval for self-regulatory guidelines. The FTC would have full authority to implement and enforce these guidelines by imposing mandatory self-regulation review and disciplinary procedures.<sup>35</sup>

To implement congressional directives, on October 20, 1999 the FTC issued the final rule to implement the **Children's Online Privacy Protection Act of 1998 (COPPA)**. Consequently, as of April 21, 2000, certain commercial websites must obtain parental consent before collecting, using or disclosing personal information on children under 13. Among the other key provisions of the final rule, sites will now be required to obtain "verifiable parental consent." The test for this will use a sliding scale by which the consent methods used by the sites will vary depending on how the information will be used. This sliding scale will be phased out in favor of more reliable methods required for all uses of information as these new methods become available.

Finally, the FTC has begun to explore the growing trend of "profiling" and its implications for privacy. For example, the FTC held a meeting on November 8, 1999 to discuss personal profiles used to facilitate more targeted online advertisements. The concern is that online privacy is compromised by "cookies" placed on consumers' home computers that allow websites to track users' online movement and compile their web preferences.<sup>36</sup> By merging these heretofore-anonymous profiles with off-line purchasing histories, advertisers can match names to profiles in order to send banner ads that will be tailored to each individual's preferences.<sup>37</sup> This new trend has consumer

---

<sup>34</sup> See Children's Online Privacy Protection Rule, 64 Fed. Reg. 22750 (1999) (to be codified at 16 C.F.R. pt. 312).

<sup>35</sup> See *id.* at 22,753-22,760 (Proposed Rule 312.4-312.10).

<sup>36</sup> See Leslie Walker, *Time to Let the Cookies Crumble*, Washington Post, Nov. 4, 1999, at E1.

<sup>37</sup> See *id.*

privacy advocates worried that such practices are an unnecessary intrusion of online personal privacy.<sup>38</sup> For its part, large online advertiser Double Click, Inc. is attempting to maintain personal privacy by refusing to use these profiling and targeting efforts on children's activities, financial, and medical records.<sup>39</sup>

## Enforcement Actions

Critical to the success of any privacy initiative is the level of enforcement, as it defines the practical parameters for privacy in the marketplace. This year, the FTC has pursued several enforcement actions that help shape privacy expectations of both consumers and business. For example, the FTC has taken action against Liberty Financial Companies, Inc., the operator of the Young Investor website featuring several areas geared toward children and teens.<sup>40</sup> The FTC's complaint alleged that the site misrepresented that visitors would receive an e-mail newsletter and prizes. In addition, the FTC alleges that the website falsely portrayed to its web users that information collected from children would be maintained on an anonymous basis. A consent agreement reached on May 6, 1999 requires Liberty Financial to post a privacy notice on its children's websites and to obtain parental consent before collecting information from children under 13.

Also notable is that on February 26, 1999, Intel released the Pentium III chip which contains a unique **Processor Serial Number (PSN)**<sup>41</sup> that is embedded in the chip to permit tracking of a user's movement on the Internet. On the same day, the Center for Democracy and Technology (CDT), Consumer Action, Privacy Rights Clearinghouse, and Private Citizen, Inc. filed a complaint with the FTC seeking immediate action to prevent harm to consumer privacy. The filing parties allege that the new PSN will detract from Internet anonymity by providing a unique identifier by which an individual can be tracked online. The complainants asked that the FTC convene an investigation into the privacy issues posed by the processor. Complainants also requested that the FTC enjoin the shipment of Intel Pentium Processors and enjoin the shipment of PSN, unless the chip is securely "off." The FTC is still investigating the complainants' allegations and has yet to determine if it will conduct formal proceedings on this matter.

According to Intel, the serial number does not "transmit" information across the web. To process the information, a website operator must purchase special software to read the processor number.<sup>42</sup> Intel argues that the PSN will enhance electronic commerce by providing enhanced security.<sup>43</sup> Never-

<sup>38</sup> See *id.*

<sup>39</sup> See *id.*

<sup>40</sup> See *In the Matter of Liberty Financial Companies, Inc.*, Case No. 982-3522 (FTC 5/6/99).

<sup>41</sup> See *In re the Matter of Intel Pentium Processor Serial Number, Complaint*, Case No. 982 (FTC 2/26/99).

theless, Intel will install a utility program that will enable the user to ascertain whether the identifier is “on” or “off.” In addition, Intel will ship the software program in the “off” position.<sup>44</sup>

Expectations are that additional enforcement actions will assist consumers and businesses in understanding the line between acceptable and impermissible practices.

## **The Clinton Administration’s Efforts**

---

Just as federal agencies have addressed issues relating to privacy and the Internet, so too has the administration. Essentially, the administration believes that government does have a role in privacy protection.<sup>45</sup>

Notably, on October 29, 1999 President Clinton and the Department of Health and Human Services released proposals designed to protect the confidentiality of patients’ online medical records, restricting the conditions under which doctors, hospitals, and health plans may divulge medical information without consent.<sup>46</sup> The recommendations, which are open for public comment for 60 days before becoming official, are divided into five key principles: (1) consumer control, which allows consumers to control how their medical records are used; (2) accountability, which describes various punishments for those who misuse health information; (3) public responsibility, which reserves the ability for unauthorized disclosure of medical records in the name of national priority; (4) boundaries, which would ensure medical records are used only for medical purposes; and (5) security, which requires those with medical information to protect it from misuse or disclosure.<sup>47</sup> The administration devised the rules after Congress failed to meet its self-imposed deadline of August 21, 1999 to pass a medical privacy law.<sup>48</sup> These proposed regulations will become law in February 2000 and will be enforced beginning in 2002.<sup>49</sup>

Other than the recent medical privacy rules, protecting the privacy of online consumers has been a challenge for the administration. The adminis-

---

<sup>42</sup> See Nadya Aswad, *Pentium III Not Likely to Violate U.S. Laws; Some Concern over EU Directive Application*, 4 *Electronic Commerce & Law Report*, No. 8, at 177 (Feb. 24, 1999).

<sup>43</sup> See *Digest*, Washington Post, Feb. 16, 1999, at E1.

<sup>44</sup> See Aswad, *supra* note 41.

<sup>45</sup> See *U.S. Government Working Group on Electronic Commerce*, First Annual Report (1998).

<sup>46</sup> Amy Goldstein, *President to Detail Patient Privacy Rules*, Washington Post, Oct. 29, 1999, at A1, A9.

<sup>47</sup> See *Protecting the Privacy of Patients’ Medical Records*, Department of Health and Human Services (Oct. 29, 1999) <<http://www.hhs.gov/news/press/1999pres/991029a.html>>.

<sup>48</sup> Goldstein, *supra* note 35.

<sup>49</sup> See *id.*

tration has maintained confidence in the industry's ability to self-regulate. In 1999, the administration has focused on the development of privacy policies for all federal websites as well as the introduction of a Financial Privacy Initiative.

To implement some measure of privacy in the federal government, and in accordance with the Privacy Act, 5 U.S.C. § 552a, the Office of Management and Budget requires all federal departments and agencies to post clear privacy policies on their websites.<sup>50</sup> Each policy must inform every visitor to the site what information the agency collects about individuals, why the agency collects it, and how the agency will use it. In addition, the privacy policy must be clearly labeled and easily accessed when someone visits the website. The departments and agencies had until September 1, 1999 to post these policies, which are mandatory on every website "point of entry" by December 1, 1999.<sup>51</sup>

With respect to emerging privacy concerns, on May 4, 1999, the administration introduced via the National Economic Council the **Financial Privacy and Consumer Protection Initiative**, an executive action to protect consumers in the new economy. The action is based upon five principles, which include: (1) protection of financial privacy; (2) expanding the consumer's right to know; (3) the prevention of fraud and abusive practices; (4) the expansion of access to financial services; and (5) the education of consumers. These principles also include proposals for credit card disclosures, allocation of law enforcement officials to resolve online financial thefts and various education programs.<sup>52</sup> The president hopes to implement this initiative before the year 2000.

Similarly, on June 23–24, 1998, the **National Telecommunications and Information Administration (NTIA)**, part of the Department of Commerce, held a two-day public meeting to explore privacy issues related to electronic commerce.<sup>53</sup> The purpose of the meeting was to discuss successful strategies for protecting privacy on the Internet, placing special emphasis on the privacy concerns of children as well as the effectiveness of self-regulation. Online industry representatives participating at this conference stressed the need to form a mutually beneficial relationship between businesses and consumers that includes choice and notice to protect and inform consumers.

The Department of Commerce, along with the Office of Management and Budget, has been also asked to report to the president on industry efforts

---

<sup>50</sup> See *Memorandum from Jacob Lew to Heads of Executive Departments and Agencies* (visited on July 20, 1999) <<http://www.whitehouse.gov/OMB/memoranda/m99-72.html>>.

<sup>51</sup> See *id.*

<sup>52</sup> See *The Clinton-Gore Plan for Financial Privacy and Consumer Protection in the 21<sup>st</sup> Century* (May 4, 1999) <<http://www.pub.whitehouse.gov/uri-res/I2R?urn:pdi://oma.eop.gov.us/1999/5/4/35.text.1>>.

<sup>53</sup> See *id.*

to establish self-regulatory regimes to ensure privacy online and to develop technological solutions to protect privacy—especially that of children.<sup>54</sup> To date, no reports have been made.

## Industry Self-Regulation

---

In an effort to curtail formal government legislation, industry officials have been developing and implementing self-regulatory policies. Since 1997, significant progress has been made to ensure that popular commercial websites post privacy disclosures. Currently, the FTC is advocating self-regulation provided that industries continue to improve their self-regulatory methods. To facilitate better this ongoing process, several organizations have created their own privacy policies and seals. The success of the following programs and others will likely be determined by consumer use and acceptance of these measures as genuine privacy assurances.

In March 1999, the **Better Business Bureau** launched a major privacy program through its subsidiary, BBBOOnLine,<sup>55</sup> to increase consumer confidence in online purchasing and reliability of online businesses. BBBOOnLine will place a “seal” on websites participating in its self-regulatory privacy efforts. This privacy seal signals customers when sensitive information is being taken, how that information will be used, and how it will be protected. Consumers will also have the option not to provide personal details such as name and phone number. Over the past two years, BBBOOnLine Reliability program has awarded 3,000 online seals to websites that meet high standards for customer satisfaction and truthful and accurate advertising. In addition, BBBOOnLine will continue to monitor participating websites for compliance as well as provide consumer dispute resolution services. Recently, on May 19, 1999, BBBOOnLine implemented a co-marketing program with several industry associations. The purpose of the program is to educate members on the BBBOOnLine Privacy Program and the importance of establishing good privacy practices in order take full advantage of the growing e-commerce market.

The **Direct Marketing Association (DMA)** has established self-regulation guidelines as well as an ethical code and for its members.<sup>56</sup> The DMA guidelines are voluntary, but the association reserves the right to suspend membership in the association for particularly egregious violations. On July

<sup>54</sup> See *Privacy Issues*, National Telecommunications and Information Administration (last modified Oct. 18, 1999) <<http://www.ntia.doc.gov/ntiahome/privacy/>>.

<sup>55</sup> See Better Business Bureau Online (last modified Oct. 27, 1999) <<http://www.bbbonline.org>>.

<sup>56</sup> See Direct Marketing Association (DMA) (last modified Oct. 29, 1999) <<http://www.the-dma.org>>.

1, 1999, the DMA implemented their “privacy promise” initiative which “raises the bar” for privacy standards.<sup>57</sup> Under this new program, the DMA requires that all DMA industry members meet their high privacy standards and they also challenge non-industry members to meet these standards.<sup>58</sup> In addition, the DMA announced that it is requiring all its members doing business in the U.S. to disclose when they are sharing consumers’ private information with other marketers.<sup>59</sup>

The **Online Privacy Alliance (OPA)** is a diverse group of companies and associations whose mission is to ensure consumer privacy in cyberspace and provide consumer education and outreach programs. In 1998, the OPA developed a framework for enforcing the protection of consumer privacy in cyberspace. The framework includes a call for objective third parties to evaluate and monitor a website’s compliance with their privacy policies. In addition, OPA has implemented consumer complaint mechanisms to adjudicate privacy violations. Furthermore, the OPA also maintains, as an integral part of its framework, a privacy “seal” program for compliant websites. To obtain this seal, the website must meet the OPA’s guidelines, including informing consumers about what personal information is being collected, how the information will be used, security for the information collected, access to that information, consent to provide such information to others, and enforcement of the privacy statement. On June 29, 1999, the OPA reported that as a result of their efforts the number of websites posting policies increased from 14% to 66% and more than 94% of the Internet’s most popular sites now maintain privacy policies.<sup>60</sup>

**TRUSTe** is an independent, nonprofit privacy organization whose mission is to build users’ trust and confidence in the Internet.<sup>61</sup> Founded by the Electronic Frontier Foundation and the CommerceNet Consortium, the TRUSTe program offers a branded online seal, or a “trustmark.” The trustmark is designed to signify to web users that the website will adhere to established privacy principles and will agree to comply with specified oversight and consumer dispute resolution processes. Currently, over 700 websites have participated in the TRUSTe program including America Online, Compaq, CyberCash, Ernst & Young, Excite, IBM, MatchLogic, Microsoft, Netscape, and Novell. TRUSTe estimates that 1,500 sites will have joined the program by the end of December 1999. In addition, TRUSTe is also working to

---

<sup>57</sup> See *id.*

<sup>58</sup> See *The DMA’s Privacy Promise*, DMA (visited July 22, 1999) <<http://www.the-dma.org/pan7/main.shtml>>.

<sup>59</sup> See *Direct Marketers Adopt New Privacy Policies*, San Jose Mercury News (July 7, 1999) <<http://www.mercurycenter.com/svtech/news/breaking/merc/docs/048331.htm>>.

<sup>60</sup> See *Online Privacy Alliance Applauds Recent Industry Efforts to Enhance Consumer Privacy Online*, Business Wire, June 29, 1999.

<sup>61</sup> See TRUSTe (visited June 25, 1999) <<http://www.truste.org>>.

develop its globally recognized seal program by maintaining licenses in all English-speaking countries and by engaging in negotiations with countries all around the world.

**CPA WebTrust** is a comprehensive seal of assurance service developed by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA). The goal of this global service is to increase consumer confidence in Internet transactions.<sup>62</sup> In order to obtain the seal, a certified public accountant (CPA) must verify that the applicant website complies with WebTrust's principles and criteria that requires a website to disclose their business practices, maintain a disclosure statement, and ensure transaction integrity and privacy. In addition, WebTrust provides a customer complaint mechanism that allows consumers to resolve complaints regarding privacy infringements, customer service, and product quality through an independent, third-party arbitrator. Currently, WebTrust is offered in the United States and several European countries.<sup>63</sup>

On July 1, 1999, **BizRocket.com, Inc.** announced the implementation of its Ethics Bureau Privacy Compliance Seal.<sup>64</sup> This seal will be awarded to websites that conform to the FTC's guidelines and display privacy statements. Features of the program include: online monitoring, dispute resolution, and privacy development programs.

The **Information Technology Industry Council (ITI)** is a group of computer manufacturers, including computer makers, chipmakers, and manufacturers of related gear.<sup>65</sup> In December 1997, ITI introduced a code of conduct for respecting privacy. These eight voluntary guidelines recommend that companies who collect data from consumers allow the consumer to choose how the data is used. ITI co-founded the Online Privacy Alliance and continues to promote other seal programs, such as BBBOnline and TRUSTe. More recently, the ITI hailed the FTC's Online Privacy Report, noting that due to increased self-regulation efforts, federal legislation would not be appropriate at this time.<sup>66</sup>

The **Platform for Internet Content Selection (PICS)** is a cross-industry working group that seeks to facilitate the development of access control technologies and software.<sup>67</sup> The technology enables individuals to define their

<sup>62</sup> See CPA WebTrust (visited June 25, 1999) <<http://www.cpawebtrust.org>>.

<sup>63</sup> See *AICPA Briefs FTC Efforts to Provide Consumer Protection in the Global Electronic Marketplace*, Business Wire, June 9, 1999.

<sup>64</sup> See *Business Ethics Bureau*, BizRocket.com (visited July 2, 1999) <<http://www.BizRocket.com>>.

<sup>65</sup> See Information Technology Industry Council (ITIC) (last modified Oct. 28, 1999) <<http://www.itic.org>>.

<sup>66</sup> See *ITI Pleads Federal Trade Commission Realizes Private Sector has made Progress in On-Line Privacy*, ITIC (July 13, 1999) <<http://www.itic.org/newsroom/index.html>>.

<sup>67</sup> See Platform for Internet Content Selection (PICS) (last modified Oct. 14, 1999) <<http://www.w3.org/PICS>>.

own privacy guidelines and to block transactions that do not comport with those guidelines. In addition, PICS offers a wide selection of products to assist parental control over their children's Internet experience.

In an effort to promote industry self-regulation, Microsoft Corporation, IBM, and Disney have announced that they will not purchase advertisements on websites that do not adhere to the FTC's guidelines, including publishing a privacy policy. IBM emphasized that consumers visiting a website: should have easy access to a company's privacy policy, should be told clearly what information is being collected and how it will be used, and should be able to elect not to provide any information.<sup>68</sup>

**Privacy International**, a human rights group formed in 1990 as a watchdog on surveillance by governments and corporations, recently joined forces with leading American privacy groups **Electronic Privacy Information Center** and **Junkbusters** to protest the merger of Internet cookie company Double Click and marketing firm Abacus Direct. The new merger "would allow the firm to personally identify net users from their cookies and create expansive profiles of their web usage."<sup>69</sup> Privacy International fears the newly merged company's ability to track people online and acquire personalized data from them without their consent based on which websites they enter will further deteriorate Internet privacy.

## International Round Up

---

Just as the United States is grappling with privacy issues, so too are international bodies. While some efforts are solely within individual countries, others are more cooperative efforts. The following provides a sampling of these efforts.

In 1981, the **Organization for Economic Cooperation and Development (OECD)** issued guidelines for the Protection of Privacy and Transborder Flows of Personal Data. These guidelines are a voluntary international standard of conduct for the collection and use of personal data. The OECD's guidelines address collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability. As the Internet has emerged, the challenge is the adaptation to today's environment.

In 1995, the Council of Ministers of the European Commission issued a **European Union (EU) Privacy Directive** ordering all member states to conform their national privacy laws with EU privacy guidelines by October

<sup>68</sup> See *IBM takes the Lead on Internet Privacy*, IBM (Mar. 31, 1999) <<http://www.ibm.com/news/1999/03/31.html>>.

<sup>69</sup> See *Privacy International Joins Protest of Invasive Internet Merger*, Privacy International (June 29, 1999) <<http://www.privacy.org/pi/>>.

25, 1998. The requirements of the EU guidelines are: (1) personal data must be collected for specific legitimate purposes; (2) data must be relevant, accurate, current, not excessive, and not be kept longer than necessary; (3) personal data may not be processed without an individual's consent, except for certain legitimate exceptions; (4) member states must provide legal remedies for breach of privacy rights; (5) member states must establish supervisory bodies to monitor national privacy policies; and (6) member states may transfer personal data to a third country if that country has adequate safeguards to protect personal data. The last item has major implications for the trans-border flow of data and has put pressure on countries outside the EU to implement their own privacy guidelines.

Since October of 1998, the **United States Department of Commerce** and the **Directorate General XV of the European Commission** have been negotiating toward the implementation of a common set of rules for data privacy on the Internet. Because the United States relies largely on self-regulation many U.S. companies are uncertain about the impact of the "adequacy" standard on personal data transfers from the European Community to the United States. To ameliorate this uncertainty, the Department of Commerce and the Directorate General are working toward the creation of a safe harbor for U.S. companies that choose voluntarily to adhere to certain privacy principles.<sup>70</sup>

The **safe harbor principles** include:

1. notice, whereby the organization must inform individuals about what type of information it collects;
2. choice, whereby the organization must give the individual the opportunity to choose whether and how their personal information is used (the "opt out" provision);
3. onward transfer, whereby the organization must require that information transferred to a third party receive the same level of privacy chosen by the individual;
4. security, whereby the organization must take reasonable measures to ensure that information be used for its designated purpose;
5. data integrity, whereby the organization must ensure that the data used is accurate, complete and current;
6. access, whereby organizations must provide individuals access to their personal information that is derived from non-public records; and
7. enforcement, mechanisms to ensure compliance with the principles, recourse for individuals and consequences for non-complying organizations.

---

<sup>70</sup> See *Draft: International Safe Harbor Principles*, Department of Commerce (Apr. 19, 1999) <<http://www.ita.doc.gov/ecom/shprin.html>>.

The United States and the European Union have resolved differences regarding the substantive aspects of the safe harbor principles. Currently, both sides are working toward resolving their procedural differences. An agreement, expected by September 1999, still has not materialized.<sup>71</sup>

The U.S. Department of Commerce recently issued an updated “discussion document” on the EU’s data privacy guidelines. The document suggests that organizations inform individuals why their personal information is being collected, tells them what to do if they have complaints, and provides an “opt out” of the collection process. In the event a company does not provide an opportunity to “opt out,” it must confirm that the third parties to which it sells the information provide adequate privacy protection. Comments on the document are due December 3, 1999.

The precise impact of these European efforts may depend upon particular countries. For example, in an effort to implement the European Union privacy directive, Italy’s Court of Auditors approved the internal organization of the **Data Protection Authority** on February 1, 1999.<sup>72</sup> This amendment to the legislative decree on privacy seeks to simplify the procedures for notification of the treatment of data in some specific areas. The decree establishes the organizational structure of the Data Protection Authority and the procedures for keeping a register of data processes. In addition, the decree creates the administrative procedures for citizen access to the register, inspections to be made by the Data Protection Authority and the filing of complaints with the Data Protection Authority.

In stark contrast to the privacy efforts made within the European Union and elsewhere, **Russia’s Federal Security Bureau (FSB)**, formerly known as the KGB, introduced a ministerial act in June of 1999.<sup>73</sup> This act would require Internet service providers to install FSB-provided “black boxes” and a hotline to the FSB that allows the FSB to monitor all electronic communications. The new act represents an addendum to an existing regulation, the System for Operational-Investigative Activities (SORM). SORM-2 is currently awaiting ministerial approval; because it is a regulation, neither President Yeltsin nor Russian Parliament will review the act.

Similarly, on September 13–15, 1999, the **Office of the Privacy Commissioner (PCO)** of Hong Kong sponsored the 21<sup>st</sup> International Conference on Privacy and Personal Data Collection.<sup>74</sup> The theme of the

<sup>71</sup> See *EU Wants Its Principles Tied to Ban on E-Commerce Tariffs*, TR Daily, Oct. 20, 1999.

<sup>72</sup> See *Regulation Adopted on Organisation of the Data Protection Authority*, European Union Legal Advisory Board News (Jan.–Feb. 1999) <<http://www.echo.lu/legal/en/lab/010299/frontpage.html>>.

<sup>73</sup> See Christopher Hamilton, *Russians Fight for Net Privacy*, ABC News (June 11, 1999) <<http://abcnews.go.com/sections/tech/>>.

<sup>74</sup> See *International Conference on Privacy and Personal Data Collection*, Office of the Privacy Commissioner (PCO) of Hong Kong (visited Oct. 15, 1999) <<http://www.pco.org.hk/info/international.html/>>.

conference was “Privacy of Personal Data, Information Technology and Global Business in the Next Millennium.” The conference, which was attended by over 50 internationally recognized speakers and panelists, covered topics ranging from the impact of current and future technologies on privacy and personal data protection to what national and international bodies are doing to provide security and privacy for consumers and businesses.

On the general issue, **Privacy International** and **Electronic Privacy Information Center (EPIC)** released their **Privacy and Human Rights 1999 survey** in September 1999. The report surveyed privacy, data protection, surveillance, and Freedom of Information Laws in over 50 countries. The report found that nearly every country in the world recognizes privacy as a fundamental human right and the most recently drafted constitutions include specific rights to access and control one’s personal information.<sup>75</sup> The report cautions that new technologies are “increasingly eroding privacy rights...[s]urveillance authority is regularly abused, even in many of the most democratic countries [and] [t]he Internet is coming under increased surveillance.”<sup>76</sup>

Privacy International also reports that in August 1999 the American company Experian revealed the financial records of up to 1.5 million South Africans on the Internet. These records included names, addresses, and identity, telephone and cell phone numbers, and bank account details on the Internet.<sup>77</sup> The records were for customers of Vodac, the Banking Council, Nedcor, First National Bank, and Standard Bank. This action further illustrates the dangers posed by new technologies to privacy and the importance of strengthening international laws governing the protection of financial and other personal information.

## Conclusion

---

As online companies and privacy advocates struggle to find a satisfactory middle ground on privacy protection, it is important to maintain a sense of the big picture. All sides support the common goal of a workable solution to these vital issues and should not lose focus of the revolutionary impact and benefits of the Internet.

The United States continues to urge industry self-regulation, with careful monitoring by the Federal Trade Commission, while the European Union maintains its path of top-down data privacy regulations. The resolution of

<sup>75</sup> See Executive Summary, *Privacy and Human Rights 1999: An International Survey of Privacy Laws and Developments* (Sept. 1999) <<http://www.privacyinternational.org/survey/summary.html/>>.

<sup>76</sup> See *id.*

<sup>77</sup> See *id.*

that ongoing debate will help shape the accessibility of global e-commerce. Other significant issues include, but are not limited to, the medical privacy rules to be released by the administration in February 2000, the FCC's CPNI rules affecting the privacy of consumer's telephone records, and the impact of the privacy provisions contained in the recently signed Financial Services Modernization Act of 1999. Again, this report provides a snapshot of the current Internet privacy issues, with new problems and proposed solutions arising every day.