

**ROOM DOCUMENT**

**Working Party on Information Security and Privacy  
Paris, OECD, 25 - 26 June 2002**

**Perspectives on Privacy Law and Enforcement Activity in the United States**

Commissioner Orson Swindle III  
United States Federal Trade Commission

Assisted by Alan Wiseman and Laura DeMartino

# **Perspectives on Privacy Law and Enforcement Activity in the United States**

**Commissioner Orson Swindle III<sup>1</sup>**  
**United States Federal Trade Commission**  
Assisted by Alan Wiseman and Laura DeMartino

## **Introduction**

The United States has been a leader in developing new technologies to support the Internet infrastructure, and electronic commerce specifically. As electronic commerce becomes more global, however, concerns have been raised over how new business models and new technologies might compromise the privacy interests of individual consumers. Some consumer advocates have argued that U.S. consumers need more commercial privacy regulation and have endorsed imposing a privacy regulatory regime on the Internet. Others state that the current legal regime is sufficient to protect consumers' privacy interests in today's evolving economy.

While not providing any concrete answers as to what kind of privacy regime (or whether any) should be imposed on the Internet, this paper provides an overview of the United States' experience with privacy. First, it discusses public concerns about privacy that accompanied the evolution of the Internet. Second, it examines existing U.S. laws that address privacy in various forums. Finally, it considers the United States' approach (and the Federal Trade Commission's (FTC) role more specifically) towards enforcing existing laws to address privacy concerns as they arise.

---

<sup>1</sup> The views expressed within this paper are those of Commissioner Swindle, and do not necessarily reflect the views of the FTC or any other individual Commissioner.

## Background

The issue of privacy has been a focus of debate for years, well before general public use of the Internet. In the United States, for example, concerns arose in the 1960s and 1970s about the government's use of citizens' personal records. The response to these concerns was the passage of legislation that would oversee information management practices at the government (public sector) level. More specifically, the Freedom of Information Act (FOIA) and the Privacy Act of 1974 prescribed (and continue to prescribe) the manner in which government agencies may collect, manage, and disclose individual records. The Privacy Act of 1974, in particular, mandates that agencies shall only collect and store information about subjects that are appropriate to their mission or task. They must also maintain the accuracy of their records and take appropriate safeguards to ensure the security of their information.

In the late 1970s and 1980s, privacy also was the focus of international discussion, as demonstrated by the promulgation of the 1980 *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* by the Organization for Economic Cooperation and Development (OECD).<sup>2</sup> The Guidelines attempt to establish best practices for the handling of personal information. They propose limits on what information may be collected, the manner in which it may be collected, and the necessity for transparency in the data-collecting and management process.

---

<sup>2</sup> O.E.C.D. Doc. (C 58 final) (October 1, 1980).

Furthermore, the Guidelines suggest that consumers and citizens have a right to have access to the information that is collected about them, and that adequate security measures should be incorporated to ensure the integrity of the relevant database. In their broadest form, the principles suggested by the Guidelines encompass what have become known as the Fair Information Practice Principles (FIPPS): Notice, Choice, Access, and Security. Since their inception, several nations have adopted the Guidelines as a model for their own commercial privacy laws, policies and practices.

As Internet usage expanded in the 1990's, so too did concerns regarding privacy. One of the defining factors that parties point to regarding how the Internet is different from conventional retail channels is the manner in which information is collected. It is often noted how the use of cookies can make passive data collection very easy for firms. They are able to monitor where potential shoppers go in their site and, when combined with certain information, to effectively uncover their preferences regarding various goods and services. While it is true that proactive business persons can engage in similar data collection in the bricks-and-mortar world by following customers around their stores, on the Internet such activities are less obvious, less costly, and more feasible on a wide scale.<sup>3</sup>

With respect to technological evolution, the use of clickstream traffic data (and other innovations) raises various privacy concerns. Most users would prefer to see advertisements or promotional offers that cater to their interests, or receive discounts on products and services that they

---

<sup>3</sup> Of course, as noted in a recent article by Ariana Eunjung Cha (*The Hovering Salesclerk is Replaced by a Computer*, *The Washington Post*, P. A01, June 16, 2002), recent developments in gaze-tracking technologies make it much easier to monitor potential shoppers' habits and tastes at bricks-and-mortar stores.

desire. Retailers argue that using clickstream data in a responsible way allows firms to provide more appropriate products to potential consumers and attract more consumers to their sites. At the same time, several privacy advocates have stated that retailers do not obtain consent to collect this data, and that the practice is needlessly invasive.<sup>4</sup> In the starkest terms, some parties have expressed fears of how corporations could amass huge treasure troves of personally-identifiable information that could be used to charge different, personalized prices between consumers or, worse yet, to discriminate against consumers in their offer of goods and services and to inevitably compromise their civil rights.<sup>5</sup>

A wide array of public opinion polls conducted over the past several years reflect consumer concerns about the use of cookies and online information collection in general. Throughout the late 1990s, the media was rife with reports of new studies that pointed to consumers and citizens being concerned about their privacy online.<sup>6</sup> A *Money Magazine* poll, from August 1997, reported that 88% of the public favored a privacy bill of rights that would require companies to tell consumers exactly what

---

<sup>4</sup> In July 2000, the FTC endorsed the Network Advertising Initiative's (NAI) Self-Regulatory Principles Governing Online Preference Marketing, which were aimed at addressing some of the above privacy concerns. See <<http://www.ftc.gov/opa/2000/07/onlineprofiling.htm>> The U.S. Department of Commerce also endorsed NAI's Self-Regulatory Principles and early on worked with companies to encourage the use of privacy policies and the development of privacy codes of conduct by online businesses.

<sup>5</sup> Testimony along these lines was heard from privacy advocates at the public workshop on "On-Line Profiling" that was co-sponsored by the Federal Trade Commission and the United States Department of Commerce on November 8, 1999. See <<http://www.ftc.gov/bcp/profiling/index.htm>> Because of efforts such as NAI's (see footnote 4), some fears of privacy advocates have not been realized.

<sup>6</sup> Information about various public opinion polls that address privacy can be found at: <<http://www.epic.org/privacy/survey>>

kind of information is collected and how it is used. Similarly, a 1997 survey conducted by the Georgia Institute of Technology's Graphic, Visualization, and Usability Center found that 72% of respondents felt that new laws were necessary to protect privacy online. These concerns remained prominent over time, as a Forrester Research survey published in September 1999 found that 67% of respondents were either "extremely" or "very concerned" about releasing personal information online.<sup>7</sup>

Privacy advocates have often pointed to these concerns as justification for new legislation that would mandate certain information management practices for the Internet. Those opposed to new legislation argue that the United States already has numerous privacy laws that can address effectively consumers' privacy concerns, without detracting from the benefits of information sharing.

### **Existing U.S. Federal Laws Concerning Information Practices and Privacy**

---

<sup>7</sup> While these results might indicate that privacy is a central concern among the American public, it is important to remember that many expressions of public opinion are highly responsive to rapid changes in one's environment. For example, in the weeks following the tragedy of September 11, 2001, a Wall Street Journal/NBC News poll found that 78% of Americans surveyed would support surveillance of Internet communications if it would contribute to greater security. More recently, in light of possible threats about a "dirty bomb" being detonated in Washington, D.C., it should be no surprise that a June 2002 poll found that 79% of Americans surveyed said that it was more important for the Federal Bureau of Investigation (FBI) to investigate possible threats than to avoid privacy intrusions.

Moreover, public opinion surveys may not predict consumers' actual behavior. As I noted in my dissent to the Commission's privacy report in 2000, "[t]he growth of online commerce despite growing consumer awareness and concern about online privacy suggests that many consumers do not act upon their fears or that they have generalized fears that are overcome by the provision of additional information by the sites with which they choose to do business." Federal Trade Commission, "Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress" (Dissenting statement of Commissioner Orson Swindle) (May 2000, p. 16).  
<<http://www.ftc.gov/reports/privacy2000/swindledissent.pdf>>.

There is no one federal law in the United States that comprehensively addresses all privacy issues. However, there are a number of existing laws that address various information practices and the privacy of consumers= personally identifiable information, both in the online and offline world. These laws provide a solid legal framework through which agencies, such as the Federal Trade Commission, can and do take enforcement actions to ensure that companies accurately represent their information management practices and that consumers= personal information is not misused.<sup>8</sup> The following list generally describes some of the statutes that pertain to privacy in the United States.<sup>9 10</sup>

### **The Federal Trade Commission Act**

The Federal Trade Commission Act, 15 U.S.C. ' 45, first enacted in 1914, empowers the Federal Trade Commission to prevent unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce. Pursuant to this mandate, the FTC can take action against

---

<sup>8</sup> Depending on the particular industry and law, other agencies might address privacy enforcement matters. For example, in addition to the FTC, several agencies that regulate the financial sector, including the Federal Reserve Board, the Office of the Comptroller of the Currency, the Office of Thrift Supervision, the Federal Deposit Insurance Corporation, the National Credit Union Administration, and the Securities and Exchange Commission enforce the privacy provisions of the Gramm-Leach-Bliley Act. Similarly, at the state level, most State Attorney Generals enforce 'like-FTC Acts' that similarly prevent deceptive or misleading statements.

<sup>9</sup> This summary is intended to provide only a broad overview of each law. The referenced statutes will provide more information about the scope and application of each law. In addition, there are other statutes that address privacy issues or regulate the use of personal data, but are not included in this summary. *See, e.g.*, Family Educational Rights and Privacy Act, 20 U.S.C. ' 1232g (applies to educational institutions= informational records), or The Drivers Privacy Protection Act, 47 U.S.C. ' 2721, *et seq.*, (regulating the disclosure of personal information contained in records maintained by state Department of Motor Vehicles).

<sup>10</sup> In addition to pertinent federal laws, states have and enforce privacy laws, including state constitutional provisions, statutes and common law torts.

companies that fail to comply with their own privacy policies or otherwise misrepresent their information management practices. The FTC also can address unfair misuse of personal information where the practice inflicts substantial harm on consumers that they cannot reasonably avoid and without offsetting benefits.

### **Title V of the Gramm-Leach-Bliley Act (GLBA)**

Section A of Title V of the GLBA, 15 U.S.C. § 6801, *et seq.*, enacted in 1999, contains privacy provisions relating to consumers' personal financial information.<sup>11</sup> Under these provisions, financial institutions have restrictions on when they may disclose a consumer's personal financial information to nonaffiliated third parties. Financial institutions are required to provide notices to their customers about their information-collection and information-sharing practices. Financial institutions also must provide consumers with an opportunity to "opt out," and stop the financial institution from sharing information with nonaffiliated third parties.<sup>12</sup> The GLBA also prohibits financial institutions from disclosing consumers' account numbers to nonaffiliated third parties for use in marketing (unless the disclosure falls within certain specific exceptions). In addition, the Act prohibits any person from using false pretenses to obtain customer information from either the financial institution or from the consumer, an abusive practice referred to as "pretexting."

---

<sup>11</sup> Each of the federal banking agencies and federal functional regulators listed above in footnote 8, are required to issue regulations that implement the GLBA. *See, e.g.*, FTC's Privacy of Consumer Financial Information Rule, 16 C.F.R. Part 313, adopted May 24, 2000; *see also* FTC's Safeguards Rule, 16 C.F.R. Part 314, adopted May 20, 2002.

<sup>12</sup> The GLBA provides specific, limited exceptions under which a financial institution may share customer information with a third party and the consumer may not opt out.

## **The Children's Online Privacy Protection Act (COPPA)**

The COPPA, 15 U.S.C. ' 6501, *et seq.*, was enacted in 1998 to protect the personal information of children under the age of 13 that is collected online.<sup>13</sup> The Act applies to operators of commercial web sites if the website is directed to children under the age of 13 or if the operators knowingly collect information from children under the age of 13. The Act prohibits web site operators from collecting, using and disclosing a child's personally identifiable information without first providing notice to the parent and obtaining verifiable parental consent. Upon request, web site operators must provide parents with access to specific personal information collected from their children and an opportunity to prevent the further use of that personal information or the future collection of information from their children.

## **Identity Theft and Assumption Deterrence Act of 1998 (Identity Theft Act)**

The Identity Theft Act, 18 U.S.C. § 1028, made it a federal crime when someone,  
. . . knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law.

The Identity Theft Act directed the FTC to establish the federal government's primary data base to collect consumer/victim reports on Identity Theft (the Identity Theft Clearinghouse, [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft)). The FTC collects complaints and provides assistance to victims by providing information to assist them in resolving financial and other problems that result from this crime.

---

<sup>13</sup> The FTC issued the Children's Online Privacy Protection Rule, 16 C.F.R. Part 312, which implements the Act.

The FTC refers victim complaints to other appropriate government agencies and private organizations for further action. Violations of the Act are investigated by the federal law enforcement agencies, including the U.S. Secret Service, the FBI, the U.S. Postal Inspection Service and the Social Security Administration's Inspector General. Federal identity theft cases are prosecuted by the U.S. Department of Justice. FTC also provides the public with consumer education materials to assist in preventing identity theft. *See, e.g.,* ID THEFT "When Bad Things Happen to Your Good Name"; ROBO DE IDENTIDAD "Algo malo puede pasarle a su buen nombre" (Federal Trade Commission, February 2002).

### **The Health Insurance Portability and Accountability Act of 1996 (HIPAA)**

The HIPAA, 42 U.S.C. ' 1320(d), and regulations issued by the Department of Health and Human Services (HHS) call for standardization of electronic patient health, administrative, and financial data, the development of unique health identifiers for all links in the health care chain (e.g., patients, employers, health plans) and the development of security standards for protecting the confidentiality and integrity of individual identifiable health information.<sup>14</sup> All health plans, healthcare clearinghouses, and healthcare providers who transmit health information in electronic form in connection with a standard transaction are affected by the law. Among the many privacy features of the legislation, HHS rules generally require (with few exceptions) covered entities to provide notice of all uses and disclosures pertaining to the personally identifiable health information collected, obtain consent before disclosing

---

<sup>14</sup> HIPAA implementing regulations are found at 45 C.F.R. Parts 160, *et seq.* (enacted in 2000 and currently subject to proposed amendment.)

that information for any purpose, and provide access to individuals to the information that has been collected about them. Patients also have a right (with a few specific exceptions) to access, inspect, and copy protected health information that was used in their treatment.

### **The Cable Communications Policy Act of 1984**

The Cable Communications Policy Act of 1984, 47 U.S.C. ' 551, sets forth subscriber privacy protections by restricting the collection, maintenance, and dissemination of subscriber information. More specifically, the Act restricts cable operators from using the system to collect personally identifiable information from consumers without prior notice and consent (which must be granted either electronically or in a written format). The Act also prohibits disclosure of personally identifiable information to third parties without consent (except for government requests pursuant to court order, or disclosures necessary for the fulfillment of cable services). Cable subscribers retain the right to inspect and correct errors in the existing database.

### **The Fair Credit Reporting Act (FCRA)**

The FCRA, 15 U.S.C. ' 1681, *et seq.*, first enacted in 1970 and amended in 1996, is designed to promote the accuracy and ensure the privacy of the sensitive financial information that is in consumer credit reports. The FCRA applies to credit reporting agencies, as well as furnishers and users of credit data. The Act allows credit bureaus to disclose consumer credit reports only to entities that have permissible purposes. If a consumer is denied benefits based on information in the report, they must be notified. The FCRA also provides consumers with the ability to access and correct information in their credit reports. In addition, consumers may opt-out of receiving prescreened offers (*i.e.*, firm, pre-approved offers of credit that are made based on information contained in their consumer reports).

## **The Federal Videotape Privacy Protection Act**

The Federal Videotape Privacy Protection Act, 18 U.S.C. ' 2710, enacted in 1988, addresses information about consumers= videotape purchases and rentals. The Act requires companies that sell or rent videotapes to obtain written consent from consumers to disclose the consumer=s personally-identifiable information (*i.e.*, information which identifies the consumer as having requested or obtained specific video material or services). Companies may disclose lists of consumer names and addresses only if they first give consumers an opportunity to opt-out of having that information disclosed.

## **Federal Trade Commission Approach**

Given that the U.S. obviously has many laws related to privacy, the question remains: how are they enforced? The FTC has taken the primary enforcement role under Section 5 of the FTC Act, the COPPA, and the FCRA and the GLBA (for certain financial institutions).<sup>15</sup> Besides enforcing existing laws, the FTC has been intensely involved in the Internet privacy debate since its genesis. Over the past several years, the Commission has studied the privacy issue, listened to the views of countless parties involved with Internet privacy (and privacy issues more broadly), and made recommendations to Congress about new legislation.

---

<sup>15</sup> The FTC also serves as the primary government enforcement backstop for the U.S.-EU Safe Harbor Framework, pursuant to its Section 5 enforcement authority under the FTC Act. The Safe Harbor Framework facilitates the free flow of data from the European Union (EU) to entities in the U.S. that self-certify to the U.S. Department of Commerce that they follow “Safe Harbor Principles” with regard to data flows of personally identifying information from the EU.

In an effort to address public concerns about privacy matters and to contribute to the general state of knowledge about privacy on the Internet, the Federal Trade Commission conducted or commissioned annual privacy surveys in 1998, 1999 and 2000.<sup>16</sup> The goal of these surveys was to identify what kinds of privacy practices were employed by online firms. More specifically, the surveys were aimed at assessing first, whether a commercial website had a privacy policy, and second, what kinds of provisions it included. For example, did a user have a choice about how their information was used? Could consumers have access to their personal information? Did the website discuss the security processes that are employed?

The results of these studies varied greatly from the first study to the last, showing an improvement in firms' privacy practices over time. In 1998, for example, only 14% of all Web sites in the FTC's comprehensive sample (674 sites) disclosed anything about their information practices, while 71% of the most popular sites provided disclosures.<sup>17</sup> The results of the 2000 survey indicated a dramatic improvement, with 88% of sites that were randomly sampled, and 100% of the most popular sites, posting at least one privacy disclosure. With respect to the provisions of notice and choice, it was noted that 41% of the random sample, and 60% of the most popular sites provided these elements to consumers on their Web sites, a stark contrast from the earlier 1998 results, when only approximately 5% of the random sample and 41% of the most popular sites had similar provisions.

---

<sup>16</sup> In 1999, Professor Mary Culnan provided to the FTC the Georgetown Internet Privacy Policy Survey, "Privacy Online in 1999: A Report to the Federal Trade Commission (June 1999).

<sup>17</sup> The "comprehensive sample" was drawn from a broader sample of more than 1400 Web sites.

Besides conducting its survey of Internet sites, the FTC also held workshops and hearings to discuss various privacy issues and regulations.<sup>18</sup> One of the more revealing forums was the Advisory Committee on Online Access and Security, which was a series of hearings held in 2000.<sup>19</sup> Drawing together a wide collection of privacy advocates, industry representatives, and academics, the advisory committee attempted to flesh out the relevant costs and benefits associated with providing consumers access to their personally identifiable information and maintaining security of the relevant databases, as well as what tools could plausibly be used to accomplish this goal. The final report of the Committee, issued in May 2000, argued that it was very difficult to quantify the costs and benefits associated with providing access to consumers, and the Committee was unable to make a strong recommendation on how such access and security should be provided.<sup>20</sup> Similar to many issues under the privacy debate, the question of how to practically implement the abstract concept of “access” proved very difficult to

---

<sup>18</sup> Among the public workshops that have been conducted by the FTC involving privacy and/or security include: the AWorkshop on Consumer Privacy on the Global Information Infrastructure@ (6/4/96), a public workshop on AConsumer Privacy Issues@ (3/4/97), a AConsumer Information Privacy Workshop@ (6/10/97), the AChildren’s Online Privacy Protection Rule Public Workshop@ (7/20/99), a public workshop on AOnline Profiling@ (11/8/99), a public workshop on the AMobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues@ (12/11-12/2000), a public workshop on AThe Information Marketplace: Merging and Exchanging Consumer Data@ (3/13/2001), an interagency public workshop on AGet Noticed: Effective Financial Privacy Notices@ (12/4/2001), and a public workshop on AConsumer Information Security@ (5/20-21/2001). Information about these workshops can be found at <<http://www.ftc.gov/privacy/reports.htm>>.

<sup>19</sup> In 1999, the FTC established the Advisory Committee on Online Access and Security to provide advice and recommendations to the Commission regarding implementation of reasonable access and adequate security by domestic commercial websites.

<sup>20</sup> “Final Report of the Federal Trade Commission Advisory Committee on Online Access and Security@ (May 15, 2000), <<http://www.ftc.gov/acoas/papers/finalreport.htm>>.

answer. Because the technology changes so quickly, it is difficult to identify a solution that might not be too restrictive or rapidly outmoded.

With respect to enforcement activities and the need for new privacy legislation, the position of the FTC has varied as the agency has learned more about the industry, self regulation,<sup>21</sup> and obtained increasing expertise with the practical problems posed by the implementation of broad based privacy legislation. Beginning with the 1998 and 1999 surveys, the Federal Trade Commission, with some disagreement among Commissioners, recommended to the United States Congress that there was no need to pass new legislation that would impose privacy regulations on the Internet.<sup>22</sup> The Internet privacy issue and the Internet industry as a whole were in their infancy and the Commission believed that the private sector would continue to make progress towards better privacy practices than what might follow from federal regulation. More specifically, to impose regulations that obviously would have nontrivial costs without clear attendant benefits, seemed inappropriate in these formative years.

The Commission's position changed in 2000, however, when the FTC formally recommended to Congress that laws should be passed that codified the Fair Information Practice Principles into

---

<sup>21</sup> Some of the most prominent self-regulatory initiatives undertaken by industry are the third-party certification seal programs such as those of TRUSTe and BBBOnline. Companies that display either of these seals guarantees to post a privacy policy on their Web sites and manage their customers' information in accordance with their posted policy.

<sup>22</sup> Federal Trade Commission, *Online Privacy: A Report to Congress* (June 1998), <<http://www.ftc.gov/reports/privacy3/index.htm>>; Federal Trade Commission, *Self-Regulation and Privacy Online: A Federal Trade Commission Report to Congress* (July 1999), <<http://www.ftc.gov/os/1999/9907/privacy99.pdf>>.

statute.<sup>23</sup> The FTC asked Congress to require that *all* consumer-oriented commercial websites provide notice, choice, access, and security to their customers. This was a dramatic policy change in the agency's position. A majority of the Commission (three commissioners) thought that insufficient progress on the part of industry had been made towards developing pragmatic and genuine privacy protections for consumers.

Although the Commission's position officially changed, two Commissioners dissented. In an extensive dissent to the Commission's report, I expressed concerns that the conclusions being reached in the report were not supported by the results from the FTC online privacy surveys. Furthermore, despite recommending new regulations, the report made no effort to account for the relative costs and benefits associated with such legislation.<sup>24</sup> In my written statement, and subsequent public statements, I have expressed fears that the broad regulatory agenda proposed in the FTC's year 2000 report could have detrimental, chilling effects on this new means of commerce. I have continued to advocate self-regulation with a government enforcement backstop. I believe that government, industry and consumer advocates working together can find mutually beneficial solutions to the privacy issues and practices causing consumers harm.<sup>25</sup> In addition, I fully support and encourage increased consumer education

---

<sup>23</sup> Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress* (May 2000), <<http://www.ftc.gov/reports/privacy2000/privacy2000.pdf>>.

<sup>24</sup> Commissioner Thomas B. Leary also dissented, in part, with the Commission report, arguing that the Commission majority's across-the-board recommendation for legislation was inappropriate given the state of the industry. *See* <<http://www.ftc.gov/reports/privacy2000/learystmt.pdf>>.

<sup>25</sup> Dissent.

and self empowerment through the use of privacy enhancing technologies (PETS). Despite the Commission's majority recommendation in 2000, no new laws have been enacted.

With the appointment of Timothy Muris as Chairman of the FTC in 2001, the Commission took a new, pragmatic direction in the privacy debate. After spending months consulting with many interests from the business, consumer and academic communities, Chairman Muris articulated his position on privacy in October 2001. The Chairman stated his belief that existing laws protecting individual privacy could and should be effectively enforced to protect consumers from the real harms caused by invasions of privacy in comparison to what might theoretically follow from new privacy regulations.

To that end, he detailed a comprehensive privacy enforcement and education agenda for the FTC as the primary consumer protection agency in the United States. Chairman Muris argued that a privacy agenda should not be restricted in focus to online information. Privacy practices and abuses offline are just as relevant in potential harm to consumers as Internet incidents. The FTC's new privacy agenda encompasses such practices as pretexting, as well as increased law enforcement coordination, education and victim assistance to deter identity theft. The new agenda also includes such issues as unsolicited commercial e-mail (spam) and telephone solicitations, practices that at many levels rely on the exchange of personal information, often contrary to the wishes of consumers. Putting forth a multi-point plan, Chairman Muris proposed pursuing numerous enforcement and education initiatives, and a 50 % increase in Commission resources devoted to privacy protection.<sup>26</sup>

---

<sup>26</sup> Remarks of Timothy J. Muris, Protecting Consumers' Privacy: 2002 and Beyond (October 4, 2001), <[www.ftc.gov/speeches/muris/privisp1002.htm](http://www.ftc.gov/speeches/muris/privisp1002.htm)>.

In terms of future enforcement activities, Chairman Muris indicated that the Commission would monitor companies' privacy practices and promises and seek to ensure that they were true to their word. He argued for increasing outreach and enforcement for children's online privacy, further enforcement of the GLBA and the FCRA, as well as additional enforcement actions against deceptive spam. The Commission would commit significant efforts towards ensuring that bad actors do not use the Internet as another venue to exploit consumers through "get-rich-quick" schemes and other familiar scams. Besides enforcing existing law, he proposed amending the Telemarketing Sales Rule to create a national, one stop, Do-Not-Call List that consumers could use if they wished to remove themselves from telemarketers' call lists.<sup>27</sup>

On the education front, the Commission would encourage consumers who had privacy complaints to file their complaints with the Commission using a specially designed complaint form at our website, [www.ftc.gov](http://www.ftc.gov). This would keep the agency alert and responsive to problems in the privacy realm. In addition, the Commission would continue to hold workshops on various privacy related matters in an effort to raise general awareness about privacy tools, practices, and problems faced by consumers and businesses.<sup>28</sup>

The new privacy agenda, especially the enforcement arm of it, was generally well-received as a positive step forward in protecting consumers' privacy interests. It was flexible enough to be effectively implemented in the quickly changing economy. Groups such as the Direct Marketing Association

---

<sup>27</sup> *Id.*

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

praised the new policy, noting that aggressively enforcing existing law would provide maximum protection and choice for consumers while not exposing business to a raft of new, costly legislation during a period of slow economic growth.<sup>29</sup> The privacy advocacy group, Electronic Privacy Information Center (EPIC), noted that it was encouraged by [Muris=] efforts to increase enforcement of existing laws; [but] disappointed on his stance on privacy legislation. Privacy scholars such as Peter Swire, the chief privacy officer for the Clinton Administration, noted that Chairman Muris was signaling now that enforcement needs to be greater, and that is consistent with the message sent by the previous Administration.

While many parties could point to the positive aspects of the FTC's new privacy agenda, many legislators, at the state and federal level, still believe that there is a need for new privacy legislation. As of June 2002, there were more than 100 bills under consideration in the United States Congress that dealt with privacy, and two bills that proposed comprehensive privacy regulation for all commercial Internet sites. Several state legislatures also have been considering various forms of privacy legislation, and one can easily imagine the patchwork of law that might emerge across the states if some sort of uniform enforcement regime is not maintained at the federal level.

### **Enforcement Actions**

The FTC has used its existing authority under the FTC Act to take action against companies that have misrepresented their information management, security, and privacy practices. The FTC has

---

<sup>29</sup> Despite its overall support, however, DMA opposes certain parts of the agenda, in particular, the proposed Do-Not-Call List.

a range of formal enforcement tools to enforce compliance with privacy requirements in the commercial realm. The FTC can issue administrative cease and desist orders barring deceptive or unfair practices. If a respondent violates an administrative order, it can be held liable for a civil penalty of up to \$11,000 for each civil violation, as well as such other and further equitable relief as is deemed appropriate. In appropriate cases, the FTC also can obtain a temporary or permanent injunction from a federal court (1) barring deceptive or unfair practices and (2) imposing various kinds of monetary equitable relief (i.e., restitution and rescission of contracts) to remedy past violations. Where applicable, the FTC also can obtain preliminary equitable relief, which may include a freeze of assets and the appointment of a temporary receiver in appropriate cases. Violations of particular statutes enforced by the FTC permit the agency to impose civil penalties and to collect funds from respondents for consumer redress. Using these powers, the FTC is aggressively enforcing provisions of the COPPA and the GLBA. Since 1999, the FTC has brought more than 30 cases involving these laws and the FTC Act. The following are just a few examples of these cases.

### **GeoCities, Inc.**

The FTC brought its first case involving Internet privacy issues against GeoCities in 1998.<sup>30</sup> GeoCities was a popular website that collected personally identifying information from consumers who became members of the site.<sup>31</sup> GeoCities' privacy policy stated that this information would only be

---

<sup>30</sup> *GeoCities, Inc.*, Docket No. C-3849 (Feb. 12, 1999). For more information, see <http://www.ftc.gov/opa/1998/9808/geocitie.htm>.

<sup>31</sup> GeoCities offered its members personal home pages and linked its members' home pages into a virtual community of themed neighborhoods. To acquire a webpage, consumers completed an online application form that asked for several items of personally-identifying information.

used to provide members with advertisements and offers that they requested, and that certain information would not be released to anyone without a consumers' permission. Contrary to its stated policy, GeoCities permitted the information to be used for purposes such as target marketing by third parties. The FTC therefore alleged that GeoCities misrepresented the purposes for which it collected personal identifying information from its customers in violation of Section 5 of the FTC Act. The FTC also alleged that GeoCities misrepresented that it alone collected and maintained personally identifying information from children. In fact, a third party actually collected and maintained that information.

GeoCities settled the charges by agreeing to post a clear and prominent Privacy Notice on its website that describes what information is being collected and for what purpose, to whom it will be disclosed, and how consumers can access and remove the information. The settlement also prohibits GeoCities from, among other things, misrepresenting the purpose for which it collects or uses personal identifying information from or about consumers. GeoCities also was required to obtain parental consent before collecting information from children 12 or younger, and to delete any such information already collected, unless it obtained affirmative parental consent to retain it.

### **Toysmart.com**

The FTC's 2000 case against Toysmart.com (Toysmart) also involved a misrepresentation of information management practices.<sup>32</sup> The company had posted a privacy policy stating that the company would never share its customers' personal information with third parties. When faced with

---

<sup>32</sup> *FTC v. Toysmart.com, LLC, and Toysmart.com, Inc.*, Civ. Action No. 00-11341-RGS (D. Mass. 2000). For more information, see <http://www.ftc.gov/opa/2000/07/toysmart2.htm>.

severe financial difficulties, however, Toysmart solicited bids for its customer lists that included or reflected the personal information of its customers. The company's creditors filed a petition to place Toysmart into involuntary bankruptcy, and the customer information was considered an asset (to be sold) of the bankruptcy estate. The FTC filed a lawsuit to prevent the sale of the customer information and alleged that Toysmart had misrepresented its privacy policy. The FTC also alleged that Toysmart violated the COPPA by collecting names, e-mail addresses, and ages of children under 13 without notifying parents or obtaining parental consent.

Toysmart agreed to settle the case, and the settlement forbids the sale of the customer information except under very limited circumstances. Specifically, the settlement mandated the terms under which the consumer information could be sold as part of Toysmart's bankruptcy estate. The consumer information could only be sold to a qualified buyer that was in a related market to Toysmart and that would abide by the terms of Toysmart's privacy statement. If the buyer sought to change that privacy policy, it would be required to obtain consumers' affirmative consent to the new uses. The negotiated settlement required Toysmart to immediately delete or destroy all information collected in violation of the COPPA.<sup>33</sup>

### **Eli Lilly and Company**

---

<sup>33</sup> FTC's settlement agreement with the respondent was not entered, for the case was dismissed when Toysmart's assets were sold and the purchaser destroyed the consumer information.

In 2002, the FTC settled a case with Eli Lilly concerning a security breach.<sup>34</sup> Lilly is a pharmaceutical company that manufactures, markets and sells several drugs, including the antidepressant medication Prozac. Lilly operated the website [www.Prozac.com](http://www.Prozac.com), which offered an e-mail reminder service. Consumers who registered for the service could receive personal e-mail messages to remind them to take or refill their Prozac medication. On June 27, 2001, a Lilly employee created a new computer program to send subscribers an e-mail message announcing the termination of the service. That e-mail included all of the recipients' e-mail addresses within the "To:" line of the message, thereby unintentionally disclosing to each individual subscriber the e-mail addresses of the 669 other subscribers.

According to the FTC complaint, Lilly claimed that it took appropriate measures to maintain and protect the privacy and confidentiality of personal information obtained from consumers on its web sites. The FTC's complaint alleged that this claim was deceptive because Lilly failed to maintain or implement internal measures appropriate under the circumstances to protect sensitive consumer information, which led to the company's unintentional disclosure of subscribers' personal information.<sup>35</sup> Lilly agreed to settle these charges.

---

<sup>34</sup> *Eli Lilly and Co.*, Docket No. C-4047 (May 8, 2002). For more information, see <http://www.ftc.gov/opa/2002/01/elililly.htm>.

<sup>35</sup> For example, Lilly allegedly failed to provide appropriate training for its employees regarding consumer privacy and information security; failed to provide appropriate oversight and assistance for the employee who sent out the e-mail, who had no prior experience in creating, testing, or implementing the computer program used; and failed to implement appropriate checks and controls on the process, such as reviewing the computer program with experienced personnel and pretesting the program internally before sending out the e-mail.

The settlement prohibits Lilly from misrepresenting the extent to which it maintains and protects the privacy and confidentiality of its consumers' information. In addition, the settlement requires Lilly to establish a security program to protect consumers' personal information against any reasonably anticipated threats or hazards to its security, confidentiality or integrity.

These cases provide a glimpse at some of the actions the FTC has taken to ensure that companies do not misrepresent their information management practices and that consumers' personal information is not misused. Appropriate enforcement of existing laws can genuinely protect consumer interests. Consistent with Chairman Muris' agenda, the Commission's enforcement activities in the privacy area will continue to be aggressive.

Case activity aside, another measure of the Commission's engagement of the privacy issue can be found in the increase in public feedback to the Commission's actions. For example, following the announcement of the proposed national Do-Not-Call Telemarketing List, the Commission received over 40,000 comments from various interests on all sides of the debate. In addition, in any given week, the Commission receives 3,000 calls from consumers who seek information or relief from identity theft or identity fraud. On matters pertaining to spam, our "spam refrigerator" at the FTC has been in existence since 1998 and currently receives more than 42,000 items of unsolicited commercial e-mail each day. A concerted effort is underway to pursue firms and individuals that have been sending fraudulent, unsolicited e-mail.

These are just a few ways in which the FTC, using the existing legal framework, is working to protect consumers' privacy by holding companies to their word. In a world in which consumers are

responsive to the posting of privacy policies and the nature of those policies, such an approach is flexible enough to allow for continuing development and innovation in the Internet economy sector, while still protecting consumers in a manner appropriate to their needs. The road ahead is long with many turns, but by working together, continuously learning from and challenging one another, business, government, and civil society will arrive at the best possible outcome.

## **Summary**

The U.S. experience with the privacy issue, proposals for comprehensive privacy legislation and law enforcement efforts is informative. This experience reveals a number of considerations that should be useful in seeking the best possible solutions for society, the economy and the future of e-commerce as the privacy debate continues.

Privacy is a concern that touches both the online and offline commercial world. Certainly, the technological advances of recent years and the ease of collecting and storing information online gives legitimate cause for concern if used improperly. However, it is important to remember that the majority of personal information is collected and stored offline, rather than online and, despite its rapid growth, e-commerce still comprises (by current estimates) only slightly more than 1% of total retail sales in the U.S. economy.

Privacy in its many variations is complex and often made more so by emotional reactions and messages. Privacy concerns, whether real or perceived, emotion-driven or not, must be addressed. One possible consequence of unaddressed concerns could be diminished confidence in the Internet and

e-commerce as new channels for economic growth. While the growth in e-commerce sales seems rapid in comparison to other commercial revolutions, complacency on the issue of privacy will surely lead to lost opportunity. This would be undesirable.

Solutions that would adequately assuage all concerns are likely to be complicated, difficult in terms of effectiveness and timeliness, and can be costly. How one arrives at solutions is not an easy problem to solve. One possible answer to this problem is the marketplace.

As public awareness of privacy issues has grown, market forces have definitely come into play. Consumers are increasingly demanding that businesses respect personal privacy and provide transparency. What consumers demand, they usually get in a free market system. In other words, good privacy practices are becoming excellent competitive tools giving one firm advantages over another because it is important to consumers. Satisfied consumers and customers are the goal of most businesses.<sup>36</sup>

---

<sup>36</sup> Although the FTC released its last online privacy study in 2000, the Progress and Freedom Foundation (PFF) conducted a follow-up study in 2001, releasing the results in 2002. The PFF attempted to assess the current state of privacy practices on the web by U.S. firms, replicating the survey methodology used by the FTC in its 2000 study. The PFF study indicated that online privacy policies became more common and more consumer-friendly in 2001. At the same time, the percentage of the most popular sites offering consumers a choice about whether their information could be shared with third parties increased from 77% in 2000 to 93% in 2001. The study also found that the privacy-enabling technology, Platform for Privacy Preferences (P3P), was being deployed rapidly.

The PFF study also considered what kinds of, and the method by which, information was being collected. It found that among the 100 most popular sites, the proportion collecting personal information actually decreased from 96% in 2000 to 84% in 2001. Even more dramatically, the proportion of those firms employing “cookies” fell from 78% to 48% in the past year. These results suggest that not all businesses, empowered with new technological tools, will seek to collect massive amounts of data. Business models and the marketplace will continue to evolve as appropriate to bring new products and services to the marketplace and to respond to consumer concerns and preferences.

The free flow of information and openness are vital to a market driven economy and bring enormous benefits to consumers. Because of the availability and flow of important personal information, many cost saving efficiencies and personal conveniences have been realized. Undue restrictions on this availability of information could have significant adverse effects on a vibrant economy.

Commercial enterprises wanting to remain competitive and successful naturally should be motivated to act in their own self-interest. Corporate leadership is increasingly more focused on the issue of respecting consumer privacy and instilling this respect through sound privacy policies and practices within the corporate culture. Progress in recent years in the development of privacy protection tools is encouraging. The development of “built-in” privacy protections for information technology and systems is still being explored. Firms are making significant investments in time, ingenuity, resources and money to best solve and minimize privacy concerns.

Surveys continue to reflect consumer concerns as well as continuing progress toward better privacy practices and policies and, as of yet, no comprehensive, far reaching privacy legislation has been passed by the U.S. Congress nor any state legislature--likely for very good reasons. The ‘Law of Unintended Consequences’ seems always in play. Experience demonstrates that often the most well-intended actions do more harm than good. The rapid expansion of e-commerce and Internet usage has

---

William F. Adkinson, Jr., Jeffrey A. Eisenach and Thomas Lenard, Progress and Freedom Foundation, *Privacy Online: A Report on the Information Practices and Policies of Commercial Websites*, <<http://www.pff.org/pr/pr032702privacyonline.htm>>.

been a product of creativity, entrepreneurship and freedom from government regulation. To unnecessarily burden its evolution with ineffective or excessive legislation is not viewed as the path to follow. Rather, narrowly focused privacy laws and regulations are being more vigorously enforced by the FTC. This will bring about an increasingly more serious attitude within the private sector for compliance with its privacy promises.

Last, the debate goes on in the U.S. as to whether comprehensive federal privacy legislation is necessary. No subject is more frequently discussed, and the effect of the dialogue illustrates the nature of market forces and informed consumers. Progress on privacy and expansion of e-commerce are evolving hand-in-hand. The countervailing forces within the society are moving the privacy issue toward better, more effective and practical solutions.

Most likely, the pattern of an informed public demanding results, combined with industry initiatives and narrowly focused government regulation and enforcement on the more sensitive privacy issues, will continue. Alternatively, comprehensive and overreaching government regulation of privacy and the Internet, as advocated by some, will likely have the chilling effect of redirecting industry efforts and resources to a “compliance mode.” Investment, creativity, and ingenuity will take a back seat to a “government solution.” An evolving problem being confronted by creative thinking and rapidly changing technology, profit-motivated investment, and good leadership will likely give way to the relatively static approach of doing what government bureaucrats and politicians decide is best. In the fast moving world of information technology, it is very unlikely that the government can keep up, regardless of good

intentions. The probable outcome of such a change in approach is to have a less effective system of privacy protection in the long run. We can and must do better than this.