

## Regulation of Privacy on the Internet in the United States

By Andre R. Jaglom\*

As the use of the Internet has become ubiquitous, companies are gathering more and more information regarding their customers and visitors to their web sites. Databases of this information are a powerful business and marketing tool, but also raise a serious threat to the privacy of personal information. Governments around the world are addressing that threat through laws regulating the collection, disclosure and use of personal data. This paper addresses recent developments in this area in the United States.

### A. Response to the European Community Directive

Use of personal data, such as medical information, credit card records, purchasing patterns and the like, by businesses that gather it, whether over the Internet or by other means, has been relatively unregulated in the United States. Except in certain specific areas, discussed below, the U.S. has adopted a laissez-faire approach to the issue. Use of such data is far more restricted in Europe, and on October 25, 1998, the European Community's Directive on "Transborder Flows of Personal Data" went into effect.<sup>1</sup> It prohibits companies from transmitting data to countries that do not adequately protect it. The Directive applies to non-European companies with European customers or employees. Thus, the collection of personal data by a U.S. company over its web site could violate European law, given the lack of formal U.S. protection of such information.

This concern was the subject of negotiations between the United States and the European Community. On July 21, 2000, the Department of Commerce issued the final draft of an intergovernmental agreement creating a "safe harbor" for U.S. companies that voluntarily and publicly agree to adhere to specified principles<sup>2</sup>, including:

(i) *Notice*: Notice to individuals of the purposes for which personal information is collected, the types of third parties to whom it is disclosed, and how individuals may limit such use and disclosure where it is for a purpose other than that for which the information was originally collected or later authorized;

(ii) *Choice*: An opportunity for individuals to choose ("opt out") whether and how their personal information is used or disclosed to third parties, where such use is incompatible with the original purpose of collection; for sensitive information (e.g. medical information or information regarding racial or ethnic origin, political

---

\* Mr. Jaglom is a member of the firm of Tannenbaum Helpert Syracuse & Hirschtritt LLP, where he practices distribution and marketing law and intellectual property law.

© 2002 Andre R. Jaglom  
All Rights Reserved

<sup>1</sup> The Directive is available at [http://europa.eu.int/smartapi/cgi/sga\\_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31995L0046&model=guichett](http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31995L0046&model=guichett) and [http://www.privacy.org/pi/intl\\_orgs/ec/eudp.html](http://www.privacy.org/pi/intl_orgs/ec/eudp.html).

<sup>2</sup> For more information on the Safe Harbor Agreement see the Commerce Department's web site at [www.export.gov/safeharbor](http://www.export.gov/safeharbor).

opinions, religious beliefs and the like, or information designated as sensitive by the source) individuals must be given an explicit choice (“opt in”) before the information is disclosed to a third party or used for a purpose other than that for which it was originally collected;

(iii) *Onward Transfer*: A requirement that third parties, who are acting as agents of the a business, to whom personal information may be transferred by that business without Notice and Choice, must provide at least the same level of protection;

(iv) *Security*: Use of reasonable measures to protect personal information from loss, misuse, unauthorized access or disclosure, alteration or destruction;

(v) *Data Integrity*: A prohibition on processing personal information in a way that is incompatible with the purposes for which it is collected or subsequently authorized;

(vi) *Access*: Giving individuals reasonable access to information about them; and

(vii) *Enforcement*: A mechanism for enforcing compliance with these principles.<sup>3</sup>

The EC has recognized the Federal Trade Commission (under §5 of the FTC Act) and the Department of Transportation (under 49 U.S.C. § 41712, relating to unfair and deceptive practices by air carriers and ticket agents) as government bodies empowered to investigate complaints and obtain relief against unfair or deceptive practices or non-compliance with the safe harbor principles.<sup>4</sup> Moreover, private damage actions have been filed in U.S. courts for the improper collection, use and transfer of personal information, albeit with little success to date.<sup>5</sup>

United States companies should consider bringing themselves within the safe harbor if they collect personal data from individuals in the EC. This means certifying to the Department of Commerce their adherence to the safe harbor principles and implementing privacy policies that comply with those principles. Many U.S. companies have been willing to take a chance and refrain signing the agreement<sup>6</sup> because not all E.U. nations had implemented the Directive and until they had done so it would be difficult for the E.U. to enforce the Directive against companies based in other countries. As of February 12, 2002, however, only Ireland and Luxembourg had yet to pass implementing legislation, and enforcement can reasonably be anticipated in the near future.

---

<sup>3</sup> See [www.ita.doc.gov/td/ecom/shprinciplesfinal.htm](http://www.ita.doc.gov/td/ecom/shprinciplesfinal.htm).

<sup>4</sup> See Jeri Clausing, “Europe and U.S. Reach Data Privacy Pact,” N.Y. TIMES, March 15, 2000.

<sup>5</sup> See, e.g., *Chance v. Avenue A, Inc.*, 165 F. Supp. 2d 1153 (W.D. Wash. 2001) (summary judgment for defendant); *In re Doubleclick Privacy Litigation*, 154 F. Supp. 2d 497 (S.D.N.Y. 2001) (summary judgment for defendant); *Rivera v. Match Logic, Inc.*, No. 00-K-2289 (D. Colo.) (filed Nov. 20, 2000), reported in 79 ANTITRUST & TRADE REG. REP. (BNA) 569 (Dec. 15, 2000); *Newby v. Amazon.com* (N.D.Cal.) (filed Jan. 7, 2000), reported at <http://news.cnet.com/news/0-1007-200-1517791.html>.

<sup>6</sup> As of September 12, 2002, there were 239 companies on the Department of Commerce’s certified list, see <http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list>.

Outside the boundary of the safe harbor, businesses that collect or receive personal data from EC persons thus risk violation of EC law, although such businesses may also elect other means of compliance, such as binding contracts with those who provide them with personal data, and anyone to whom they transfer such data, that conform to EC Directive requirements. The EC has adopted standard contract forms for this purpose, under which the data transferred are treated in compliance with EU data protection standards.<sup>7</sup>

## **B. U.S. Online Privacy Regulation Generally**

### **1. The 1998 and 1999 Federal Trade Commission Privacy Report**

Recent events suggest that the American laissez-faire approach has begun to change, albeit slowly. The Federal Trade Commission in June 1998 issued “Privacy Online: A Report to Congress” (hereafter, the “1998 Privacy Report”).<sup>8</sup> That report asserts as four core principles of fair information practice: “that consumers be given *notice* of an entity’s information practices; that the consumers be given a *choice* with respect to the use and dissemination of information collected from or about them; and that the consumers be given *access* to information about them collected and stored by an entity; and that the data collector take appropriate steps to insure the *security* and integrity of any information collected.”<sup>9</sup>

In connection with the 1998 Privacy Report, the FTC examined the practices of over 1,400 web sites and found that they fell short of adequately protecting consumers even as to the most basic of the above principles – notice. The FTC found that over 85% of the sites collected information from consumers, but only 14% provided any notice of their information practices, and only 20% did so through a comprehensive privacy policy. Even on children’s sites, 89% collected information from children, and few provided for any meaningful parental involvement. 54% of children’s sites provided some notice of their information practices, but only 23% told children to seek parental permission before providing personal information.<sup>10</sup> The FTC recommended legislation to protect children’s information, enacted as the Children’s Online Privacy Protection Act (“COPPA”), discussed below.

A year later, in July 1999, the FTC issued a subsequent report, “Self-Regulation and Privacy Online: A Report to Congress” (the “1999 Privacy Report”),<sup>11</sup> which continued to support self-regulation of privacy issues outside of the context of children’s personal information. The 1999 Privacy Report noted significant progress since the 1998 Privacy Report, but also significant remaining challenges in implementing the core principles described above. The 1999 Privacy Report concluded again that no legislation to address on-line privacy generally was required for the time being, but found a need for industry to encourage widespread adoption of fair information practices, and to educate consumers about privacy protection on the Internet. The FTC indicated it would monitor

---

<sup>7</sup> See [www.europa.eu.int/comm/privacy](http://www.europa.eu.int/comm/privacy); WORLD DATA PROTECTION REP. (BNA) (Feb. 2002) at 4.

<sup>8</sup> See [www.ftc.gov/reports/privacy3/priv-23a.pdf](http://www.ftc.gov/reports/privacy3/priv-23a.pdf).

<sup>9</sup> 1998 Privacy Report at ii (emphasis in original).

<sup>10</sup> *Id.* at iii.

<sup>11</sup> See [www.ftc.gov/os/1999/9907/privacy99.pdf](http://www.ftc.gov/os/1999/9907/privacy99.pdf).

the development of “privacy seal” programs, such as TRUSTe, which permit a web site operator to display a program’s seal, providing it agrees to meet specified privacy standards and be subject to enforcement mechanisms.

In addition, in August 1998, the FTC settled its first Internet privacy charges, alleging that GeoCities collected personal data on its web site pursuant to a stated policy that restricted its use, and then failed to honor that policy.<sup>12</sup> GeoCities agreed to place a clear privacy policy notice on its site, informing consumers of what information was being collected and for what purpose, stating to whom data would be disclosed, and informing consumers how they could access and remove the data. Parental consent would be required before information from children 12 and under could be collected.

## 2. The 2000 FTC Recommendations

On May 22, 2000, the FTC released its third report to Congress dealing with self-regulation with respect to online privacy and other issues.<sup>13</sup> For the first time, the FTC concluded by a 3-2 vote that, while self-regulation by online companies has been improving, it was unlikely to attain a high enough level to satisfy consumers without legislation. Chairman Robert Pitofsky discussed the four elements of privacy protection, now widely known as the Fair Information Practice Principles:<sup>14</sup>

(i) *Notice*: Provide consumers with clear and conspicuous notice of the site’s information practices, including what information it collect, how it collects it (such as a direct method or through non-obvious cookies<sup>15</sup>), how it uses it, how they provide Choice, Access, and Security to consumers, whether they disclose the information collected to other entities, and whether other entities are collecting information through the site.

(ii) *Choice*: Offer consumers choices as to how their personal identifying information is used beyond the use for which the information was provided (such as to consummate a transaction). Such choices would encompass both internal secondary uses (such as marketing back to consumers) and external secondary uses (such as disclosing data to other entities).

(iii) *Access*: Offer consumers reasonable access to the information the site has collected about them, including a reasonable opportunity to review the information and to correct inaccuracies or delete information.

---

<sup>12</sup> GeoCities, TRADE CAS. (CCH) ¶ 24,485 (1998).

<sup>13</sup> See [www.ftc.gov/reports/privacy2000/privacy2000.pdf](http://www.ftc.gov/reports/privacy2000/privacy2000.pdf).

<sup>14</sup> See [www.ftc.gov/os/2000/10/pitofskystatement.htm](http://www.ftc.gov/os/2000/10/pitofskystatement.htm).

<sup>15</sup> *But see In re DoubleClick Inc.*, 154 F. Supp. 2d 497 (S.D.N.Y. 2001) (ruling that the use of cookies to gather information about web surfers does not violate federal privacy statutes). On May 30, 2002, the European Union Parliament approved a Directive concerning the processing of personal data and the protection of privacy in the electronic communications sector, which contains a provision stating that invisible tracking devices, such as cookies, may be employed only after a user is provided with adequate information about the purpose of such tracking device and has the opportunity to reject such device. It is expected that this Directive will be in effect and applied by the end of 2003. *EU Commission Welcomes European Parliament’s Vote to Accept Directive on Data Protection Rules for Electronic Communications Sector*, EU Press Release May 30, 2002, located at <http://www.eurunion.org/news/press/2002/2002034.htm>.

(iv) *Security*: Take reasonable steps to protect the security of the information the site collects from consumers.

Based on the results of a survey by the FTC of the busiest commercial U.S. web sites that found only 20% of the web sites in the sample implemented all four of the suggested principles, FTC Chairman Pitofsky, speaking for a majority of the Commission, declared that “self-regulation alone, without some legislation, is unlikely to provide online consumers with the level of protection they seek and deserve.”

The legislation that the FTC suggested in 2000 would have established a ground-level amount of privacy protection similar to that which is provided for children by COPPA. Without overlapping the COPPA guidelines, the legislation would have covered the same four widely accepted Fair Information Principles.

### 3. Recent FTC Developments

With the replacement of Robert Pitofsky in 2001 by new FTC Chairman Timothy Muris, who has indicated a preference for greater enforcement of existing law, rather than more legislation, the balance shifted back. One year ago, Chairman Muris outlined the FTC’s current and future privacy initiatives and announced the FTC’s plan to increase resources devoted to protecting consumer privacy by 50%.<sup>16</sup> Among the issues on the FTC’s pro-privacy agenda are enforcing the privacy promises posted on web sites,<sup>17</sup> investigating complaints of U.S. companies failing to provide privacy protections they had promised under the European Safe Harbor Principles and encouraging strong security for personal information collection. Chairman Muris concluded by stating that although broad-based online privacy legislation could be beneficial, it is too soon to be able to fashion workable federal legislation and more law enforcement, not more laws, should be the FTC’s focus now.<sup>18</sup> While there have been privacy bills introduced in Congress this year, none have yet been enacted. In the short term, the states may increase their regulatory efforts, thereby creating a patchwork of conflicting legislation – the very thing proponents of federal regulation had hoped to avoid.<sup>19</sup>

After the events of September 11, 2001, the U.S. government has been focused on security, including on-line security. Chairman Muris’s position that no new privacy laws are needed complements existing and proposed laws which seek to curtail users’ right to privacy in the interest of national security and an increase in the U.S. government’s

---

<sup>16</sup> *Protecting Consumers’ Privacy: 2002 and Beyond: Remarks of FTC Chairman Timothy J. Muris*, at The Privacy 2001 Conference, Oct. 4, 2001, located at <http://www.ftc.gov/speeches/muris/privisp1002.htm>.

<sup>17</sup> One example of such a case is noteworthy because of its bankruptcy context. The FTC sued to enjoin the bankrupt Toysmart from selling, in bankruptcy, its customers’ personal information in violation of its privacy policy promise never to share that information. *FTC v. Toysmart.com*, Civ. No. 00-1134-RGS (D. Mass., filed July 10, 2000). A settlement would have permitted transfer of the customer data to a purchaser who bought the entire business; otherwise, the data was to be destroyed. The bankruptcy court did not approve the settlement, finding it unduly restrictive, but left the door open for objections, the FTC once a potential buyer was on the scene.

<sup>18</sup> *Protecting Consumers’ Privacy: 2002 and Beyond, supra*. In concluding that now is not the time for broad-based online privacy legislation the Chairman cited the general experience under the Gramm-Leach-Bliley Act, “a digital mattress tag” under which “[a] cres of trees died to produce a blizzard of barely comprehensible privacy notices.”

<sup>19</sup> See John Schwartz, *F.T.C. Plans To Abandon New Bills On Privacy*, N.Y. TIMES (Oct. 3, 2001), at C5.

ability to conduct on-line surveillance. This may be a dangerous combination for privacy, as evidenced by companies that have handed to the government entire databases in violation of their own privacy policies<sup>20</sup> in an effort to assist with terrorist investigations.<sup>21</sup>

Recent FTC activities have included an announcement that, in the absence of clear statements to the contrary, a company's online privacy policy would be considered to apply equally to a company's offline collection and use of data.<sup>22</sup> And in early 2002, the FTC settled an action against Eli Lilly and Co. for alleged inadvertent violation of its privacy policy.<sup>23</sup> A Lilly employee had unintentionally sent an e-mail to all subscribers to a Prozac-related e-mail service, placing their e-mail addresses in the "To:" field, and thereby making the addresses visible to all. The FTC charged that Lilly's inadequate internal security procedures rendered its privacy policy deceptive. The settlement required implementation of a security program to protect consumer's personal information from reasonably foreseeable threats to its security, confidentiality or integrity and from unauthorized access, use or disclosure.

Later in 2002 the FTC settled charges with Microsoft that alleged that it had misled consumers as to the security and privacy of personal information in its Passport online authentication system.<sup>24</sup> While no actual security breaches had been found in the FTC's investigation, the security claims that Microsoft had made were not substantiated – a standard like that for any advertising claims. The FTC in both the Lilly and Microsoft cases required designated personnel to be responsible for information security, identification of security risks, implementation of security safeguards to control those risks and ongoing monitoring of the security program for effectiveness.<sup>25</sup> Similar approaches appear in the information security guidelines adopted as Recommendations by the Organization for Economic Cooperation and Development Council on July 25, 2002<sup>26</sup> and the FTC's final rule establishing information security standards for customer information under the Gramm-Leach-Bliley Act.<sup>27</sup>

These recent developments demonstrate that a company's consumer privacy initiatives cannot begin and end with the issuance of a privacy policy. Businesses must actively review and monitor their offline and online privacy programs and take

---

<sup>20</sup> Companies typically require a warrant or court order before relinquishing the contents of electronic files to the government. Companies may soon look to rewrite their privacy policies to include provisions that would enable them to make records available to the government in the event of a national emergency. Stefanie Olsen, *Companies rethink Net privacy after attacks*, CNET.COM (Oct. 2, 2001), located at <http://news.com.com/2100-1023-273767.html>.

<sup>21</sup> Janine Canham, *Security on the Internet – At the Cost of Privacy?*, WORLD INTERNET L. REP. (BNA) (Nov. 2001), at 34.

<sup>22</sup> See WORLD DATA PROTECTION REPORT (BNA) (January 2002) at 17.

<sup>23</sup> *In re Eli Lilly and Co.*, FTC No. 0123214 (Jan. 18, 2002) reported in WORLD DATA PROTECTION REP. (BNA) at 12.

<sup>24</sup> 83 Antitrust & Trade Reg. Rep (BNA) 137, 193 (2002). The European Commission had undertaken a similar investigation. "Microsoft Faces European Commission Inquiry on Privacy Concerns," N.Y. Times (May 28, 2002) at p. C4.

<sup>25</sup> *Id.* at 194.

<sup>26</sup> See [www.oecd.org/EN/document/0,,EN-document-43-1-no-24-33185-0,00.html](http://www.oecd.org/EN/document/0,,EN-document-43-1-no-24-33185-0,00.html).

<sup>27</sup> See [www.ftc.gov/opa/2002/05/safeguardrule.htm](http://www.ftc.gov/opa/2002/05/safeguardrule.htm).

appropriate measures to preclude unauthorized access to or dissemination of its customers' private information, even inadvertently.

#### **4. State Privacy Protection**

Privacy regulation is not limited to the federal level. The States have entered the arena as well, both with new legislation and enforcement actions. In 2002, for example, Minnesota and North Dakota enacted new privacy laws. The Minnesota statute requires internet service providers to inform Minnesota customers if they plan to disclose personal information, including e-mail and physical addresses, telephone numbers and web sites that the customer visited, what the information would be used for, and how the customer could act to prevent the disclosure, whether on an opt-out or opt-in basis.<sup>28</sup> North Dakota voters overwhelmingly voted in June 2002 to repeal a 2001 law allowing financial institutions to share customer data unless the customer opted out, reinstating an opt-in regime in which advance permission to share information was required.<sup>29</sup> Vermont and New Mexico have also adopted opt-in standards.<sup>30</sup>

On the enforcement side, DoubleClick, an on-line advertising company, settled an investigation by ten state attorneys general by accepting tight privacy restrictions and paying \$450,000 to cover the States' investigative costs. DoubleClick had tracked users' web-surfing by means of cookies – small files placed on the user's computer – allowing it to select the ads to display based on the user's preferences. The settlement requires DoubleClick to give users access to their profiles maintained by DoubleClick and imposes restrictions on the use of the information it gathered.<sup>31</sup>

#### **C. Specific Areas of Regulation**

##### **1. Privacy of Children's Personal Information – COPPA**

As a result of the 1998 Privacy Report, the FTC recommended greater incentives for industry self-regulation and proposed legislation regulating the collection and use of information from children. Such legislation was enacted in October 1998. The Children's Online Privacy Protection Act of 1998<sup>32</sup> required the FTC to issue regulations governing operators of web sites and online services who know they are collecting personal information from children under the age of 13 and provided for enforcement actions by the FTC and state attorneys general.

---

<sup>28</sup> Minn. Laws 2002, ch.395; for text see [www.spamlaws.com/state/mn.html](http://www.spamlaws.com/state/mn.html).

<sup>29</sup> N.D. Century Code §6-08.1-01. See "North Dakota Tightens Laws on Bank Data and Privacy," N.Y. TIMES, June 13, 2002 at A286.

<sup>30</sup> Vt. Dep't of Banking, Insurance, Securities & Health Care Admin., Banking Div'n Regulation B-2001-01 (Privacy of Consumer Financial and Health International Regulation). For text see [http://www.bishca.state.vt.us/Regs&Bulls/bnkregs/REG\\_B2001\\_01.pdf](http://www.bishca.state.vt.us/Regs&Bulls/bnkregs/REG_B2001_01.pdf). See generally J. Plummer, "Mandating Opt-In May Cause Consumers to be Left Out," <http://www.nccprivacy.org/online/CR0205.htm>.

<sup>31</sup> "DoubleClick Settles Privacy Inquiry," N.Y. TIMES (Aug. 27, 2002) at C3.

<sup>32</sup> 15 U.S.C. §§ 6501 *et seq.*

The FTC issued the required regulations on October 20, 1999,<sup>33</sup> requiring a clear and prominent list on a web site's home page and each page where personal information is collected from children, stating the name and contact information of each operator of the site, the types of personal information collected, how it is used and whether it is disclosed to third parties. The notice must state that a child's participation in an activity may not be conditioned on disclosing more information than is reasonably necessary, and that a parent can review a child's personal information, have such information deleted and refuse to permit further collection or use of the child's data. By 2001, 91% of children's web sites posted privacy policies, compared with only 24% in 1998.<sup>34</sup>

The regulations adopted a sliding scale for parental consent, initially for two years, but extended earlier this year to April 21, 2005. A reliable method of consent is required for activities that pose the greatest risk to children, such as disclosing personal information to third parties or making it publicly available in chat rooms. Examples of such methods include mailing or faxing a signed printout, use of a credit card or a toll-free number, digital signatures, and email with a PIN or password. For internal uses of information, such as marketing back to the child, e-mail consent is sufficient, so long as additional steps are taken to confirm that the parent is providing consent. Eventually, the more reliable methods of consent will be required for all uses, unless the Commission determines otherwise. Parents must be given the option of permitting the collection and use of the child's personal information without consenting to disclosure to third parties. The rule also provides for certain exceptions to the prior consent requirement, and for a "safe harbor" program for industry groups who create self-regulatory programs approved by the Commission.

In May 1999, before issuance of the regulations, the FTC settled charges against Liberty Financial Companies, Inc. alleging that the company solicited information from children and teenagers on the representation that the information would be totally anonymous, when in fact it was maintained in a database in identifiable form.<sup>35</sup> The settlement prohibited Liberty Financial from making misrepresentations about its collection of personal information from children under 18, and from collecting personal information from children under 18 if it knows the child does not have parental consent to provide it. The settlement further requires prominent notice regarding the collection and use of information, a procedure for obtaining verifiable parental consent and deletion of all information previously collected from children.

In its first enforcement action under COPPA, the FTC imposed fines totaling \$100,000.<sup>36</sup> The FTC has continued to be active in its protection of children's privacy, filing four civil penalty actions in 2001 to enforce COPPA and pursuing active investigations on additional matters.<sup>37</sup> The FTC settled a case against a company which

---

<sup>33</sup> 16 CFR Part 312 (1999); TRADE REG. REP. (CCH) No. 575 Part 2 (April 28, 1999).

<sup>34</sup> *3 Web Operators Settle COPPA Charges For Unauthorized Collection of Personal Data*, 80 ANTITRUST & TRADE REG. REP. 2004 (BNA) (Apr. 20, 2001), at 357.

<sup>35</sup> *Liberty Financial Companies, Inc.* TRADE CAS. (CCH) ¶ 24,598 (1999).

<sup>36</sup> Henry Beck & Victoria Guest, *Violations of COPPA continue*, THE NAT'L L.J. (Aug. 20, 2001) (the web sites fined were girlslife.com, insidetheweb.com and bigmailbox.com).

<sup>37</sup> *Protecting Consumers' Privacy: 2002 and Beyond: Remarks of FTC Chairman Timothy J. Muris*, at The Privacy 2001 Conference, Oct. 4, 2001, located at <http://www.ftc.gov/speeches/muris/privisp1002.htm>.

was using its web site to target young girls and which, after having been warned, continued to collect information from underage girls in violation of COPPA. The company paid \$30,000 as a civil penalty and is barred permanently from committing future violations of COPPA.<sup>38</sup>

More recently, in April 2002, the FTC settled charges against the Ohio Art Co., the makers of Etch-A-Sketch, alleging that it collected names, addresses, e-mail addresses and birth dates from children registering for “Etchy’s Birthday Club”. Ohio Art instructed the children to “get your parents or guardian’s consent first,” but did nothing to verify parental consent. The FTC also charged that Ohio Art collected more information than was necessary for participation in the “club” and that its privacy policy did not comply with COPPA’s requirements. The settlement required a \$35,000 civil penalty and the deletion of all personal information improperly collected for the past two years.<sup>39</sup>

The FTC has issued more than 50 warning letters to the operators of children’s web sites for non-compliance with COPPA.<sup>40</sup>

## **2. Financial Services – The Gramm-Leach-Bliley Act**

### *a. Privacy Regulation*

The 1999 Gramm-Leach-Bliley Act, which deregulated the financial services industry, imposed privacy regulations on any company that engages in financial activities under the Bank Holding Company Act of 1956. These activities cover a broad range of companies, potentially including all companies that extend credit to consumers. Title Five of the Act contains the Act’s privacy provisions, which protect nonpublic personal information of natural persons (whether gathered offline or online), require disclosure of privacy policies in specified areas and restrict the disclosure or sharing of such information with third parties.

This Act requires “financial institutions” to establish privacy policies and disclose these policies when they first begin a relationship with a customer and then yearly after that. It also requires these institutions to give to customers the right to decide whether they want to block the sharing of their confidential information with other third parties. In effect, the Act uses an “opt-out” provision for certain non-public information.

These financial institutions are unconditionally barred from sharing credit card or other account numbers or access codes of customers with third parties for the purpose of direct mailings, telemarketing or Internet marketing. “Financial Institutions” are defined with respect to the guidelines in Section 4(k) of the Bank Holding Company Act. Activities included within the Act include lending, insurance underwriting and sales, as well as securities underwriting and sales. Companies engaging in these activities – not only banks – are subject to these privacy provisions of the Gramm-Leach-Bliley Act.

---

<sup>38</sup> *Manufacturer of Popular Girls’ Toys Settles FTC Charges of Violating COPPA*, 81 ANTITRUST & TRADE REG. REP. 2027 (BNA) (Oct. 5, 2001).

<sup>39</sup> 82 ANTITRUST & TRADE REG. REP. (BNA) 365 (April 26, 2002); *eSchool News online*, <http://www.eschoolnews.com/news/showStory.cfm?ArticleID=3744&ref=wo>.

<sup>40</sup> 82 ANTITRUST & TRADE REG. REP. (BNA) 365 (April 26, 2002).

The provisions of the Act were phased in over time. The Act gave most affected business six months to issue and disclose their privacy policies.

In addition, the Gramm-Leach-Bliley Act designated specific federal regulatory agencies to oversee the implementation of Title Five in particular sectors of the financial industry. The Federal Trade Commission has jurisdiction over financial institutions that are not otherwise regulated by another federal regulatory body.<sup>41</sup>

On May 15, 2000, the FTC issued a final Rule on the implementation of the Gramm-Leach-Bliley Act. This Rule imposed the requirements generally called for by the Act:

- A “financial institution” must provide to its customers a clear and conspicuous notice about its privacy policies and practices. The notice must describe when and where the “financial institution” may disclose nonpublic information to unaffiliated third parties.
- A “financial institution” must also provide to its customers a clear and conspicuous annual notice of its privacy policies.
- Finally, a “financial institution” must provide its customers with a reasonable chance to “opt out” of disclosures of their nonpublic information to unaffiliated third parties. This opt out must be available at all times.

The deadline for full compliance with the FTC Rule was July 1, 2001.

#### *b. FTC Enforcement*

In June of 2000, the FTC entered into a settlement with two information brokers who violated §5 of the FTC Act by “pretexting” (lying about their identity to obtain private financial information about individual consumers from financial institutions) in a deceptive manner. The proposed settlement barred the brokers from engaging in future deceptive practices and also prohibited them from “pretexting,” “except where permitted by the Gramm-Leach-Bliley Act.” In addition, the brokers were required to post a privacy policy on their web site, disclosing the information they are collecting. This is one of the first reported cases to implement the Act in a forward-looking settlement. Over the following year the FTC examined hundreds of web sites and ads for companies offering financial services and issued over 200 warning letters and commenced several federal court actions for pretexting.

#### *c. The Safeguards Rule*

As part of its implementation of the Gramm-Leach-Bliley Act, in May 2002, the FTC issued final rules implementing Section 501(b) of the Gramm-Leach-Bliley Act (the “Safeguards Rule”).<sup>42</sup> The purpose of the Safeguards Rule is to establish standards

---

<sup>41</sup> Other regulators include the SEC, the CFTC, the Comptroller of Currency, the Board of Governors of the Federal Reserve System, the Board of Directors of the Federal Deposit Insurance Corporation, the Directors of the Office of Thrift Supervision, the Board of the National Credit Union Administration, and state insurance regulators. These agencies have issued similar regulations.

<sup>42</sup> See Standards for Safeguarding Customer Information; final rule, 16 C.F.R. 314; “FTC Issues Financial Information Safeguards Rule,” FTC Release (May 17, 2002). See also Federal Trade Commission –

relating to administrative, technical and physical information safeguards as required by Section 501(b) of the Gramm-Leach-Bliley Act. Such standards are intended to ensure the security and confidentiality of customer records and information, to protect against any anticipated threats or hazards to the security or integrity of such records, and to protect against unauthorized access to or use of such records on information that could result in substantial harm to a customer.

Pursuant to the Safeguards Rule, a financial institution must adopt a written information security program (“ISP”).<sup>43</sup> With respect to its ISP, a financial institution must cover the following five elements:

- Designate an employee or employees to coordinate the ISP;
- Conduct risk assessment to identify internal and external risks to security, confidentiality and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction of such information. Moreover, the FTC considers three areas to be the “most relevant” when conducting risk assessment: (i) employee training; (ii) information systems design, processing, storage, transmission and retrieval; and (iii) preventing, detecting and responding to attacks, intrusions or system failures;
- Design an ISP and detail the plans to monitor the ISP;
- Require third-party service providers that a financial institution has retained, by contract, to implement and maintain information safeguards; and
- Evaluate and adjust the ISP in light of changes to a financial institution’s business operations or the results of its monitoring and security tests.<sup>44</sup>

The fourth element requires a financial institution to ensure that its third-party service provider comply with the Safeguards Rule if such a service provider receives a customer’s nonpublic personal information.<sup>45</sup> Pursuant to the Safeguards Rule, a financial institution must require its service provider, *by contract*, to implement and maintain information safeguards. As such, a financial institution will have to review an administrator’s information operations and then negotiate and enter into a contract that obligates an administrator to adopt the same provisions under the Safeguards Rule. How administrators will react to this regulatory burden remain to be seen.

Financial institutions must implement their ISPs by May 23, 2003.<sup>46</sup> As such, financial institutions have the next seven months to evaluate their operations and to develop an ISP. Furthermore, there is a transition rule for contracts entered into by June

---

Business Alert, “Safeguarding Customers’ Personal Information: A Requirement for Financial Institutions,” available at <http://www.ftc.gov/bcp/online/pubs/alerts/safealrt.htm>.

<sup>43</sup> See 16 C.F.R. 314.3(a).

<sup>44</sup> See 16 C.F.R. 314.4(a)-(e).

<sup>45</sup> See 16 C.F.R. 314.4(d)(2).

<sup>46</sup> See 16 C.F.R. 314.5(a). See also FTC Commentary to 16 C.F.R. 314. The Safeguards Rule will take effect one year from the date on which the final rule is published in the Federal Register which was May 23, 2002. See FTC Commentary to 16 C.F.R. 314.

23, 2002 between financial institutions and third-party service providers.<sup>47</sup> This transition rule gives financial institutions two years to require its service providers, by contract, to implement an ISP.<sup>48</sup> Accordingly, financial institutions have until May 23, 2004 to bring service contracts with administrators into compliance with the Safeguards Rule. To assist financial institutions in complying with the Safeguards Rule, the FTC will issue guidance on how to implement and monitor an ISP and on how to oversee a third-party service provider in the near future.<sup>49</sup>

### 3. Medical Records – HIPAA

Privacy of individually identifiable health information is regulated by the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”)<sup>50</sup> and regulations promulgated under HIPAA.<sup>51</sup> HIPAA regulates “covered entities, which include health care providers, health plans and “health care clearinghouses”<sup>52</sup> that maintain or transmit health information using electronic media.

Under the original HIPAA regulations adopted at the end of the Clinton administration, use of an individual’s health information required the individual’s consent, regardless of the use. Consent was required before medical data could be used for treatment, payment, marketing or a variety of other activities.

Under new regulations issued by the Bush administration in August 2002,<sup>53</sup> the requirement of consent for treatment and reimbursement was eliminated, replaced by mere notice by the covered entity of its disclosure policies. The Bush administration argued that the consent requirement could delay treatment. Although consent is still nominally required for marketing activities, the new regulations distinguish recommending treatment from marketing, a loophole exploited by pharmaceutical companies paying pharmacies to send mailings advocating the use of alternative proprietary drugs to patients that the pharmacy records indicate use competing products, without the knowledge or consent of the patients.<sup>54</sup>

Employee health plans are generally subject to the privacy restrictions, although there are exceptions for fully insured plans and self-administered plans with fewer than fifty participants. Where an employer is not a covered entity, but its health plan is, it is

---

<sup>47</sup> See 16 C.F.R. 314.5(b). See also FTC Commentary to 16 C.F.R. 314. Contracts between financial institutions and nonaffiliated third-party service providers are given two years to bring service provider contracts into compliance with the Safeguards Rule as long as the contract was in place 30 days after the date on which the final rule was published in the Federal Register which was May 23, 2002. See FTC Commentary to 16 C.F.R. 314.

<sup>48</sup> See 16 C.F.R. 314.5(b). See also FTC Commentary to 16 C.F.R. 314.

<sup>49</sup> See FTC Commentary to 16 C.F.R. 314.

<sup>50</sup> Pub.L.No.104-191, 110 Stat. 1936 (1996).

<sup>51</sup> 45 C.F.R. Parts 160 and 164.

<sup>52</sup> A health care clearinghouse is “a public or private entity that processes or facilitates the processing of nonstandard run data elements of health information into standard data elements.” 42 U.S.C. § 1320(d)(2).

<sup>53</sup> 45 C.F.R. Parts 160 and 164.

<sup>54</sup> A. Zimmerman & D. Armstrong, “How Drug Makers Use Pharmacies To Push Pricey Pills,” *The Wall Street Journal*, p.A1 (May 1, 2002).

important to create appropriate firewalls to keep the health plan's information from the employer.

#### 4. Workplace Privacy

In the United States, employees' privacy rights have been severely curtailed through the virtually unregulated and unrestricted use of various electronic monitoring and surveillance systems utilized by employers. Up to 14 million U.S. workers are subject to continuous surveillance of their e-mail and Internet use while at work.<sup>55</sup> As a general rule, employees do not have an expectation of privacy from their employer in their e-mail or office systems, particularly where the employer has an announced policy of monitoring e-mail.<sup>56</sup>

The announced policy is important, however, to avoid falling under the Electronic Communications Privacy Act of 1986<sup>57</sup> – the federal wiretap law – which bars third party interception electronic communications. The Act contains an exception for an employer's right to monitor employees, provided it is done in the ordinary course of business or with the employee's express or implied consent. It thus is important for employers who wish to monitor e-mail to provide notice of a policy that negates any expectation of privacy by employees in their e-mail.

---

<sup>55</sup> See, Carl S. Kaplan, *Reconsidering the Privacy of Office Computers*, N.Y. TIMES ON-LINE, (July 27, 2001), located at <http://www.nytimes.com/2001/07/27/technology/27CYBERLAW.html>.

<sup>56</sup> See, e.g., *McLaren v. Microsoft Corp.*, No. 05-97-00824-cv (Tex. Ct. App. 1999); *Smyth v. Pillsbury Co.*, 914 F. Supp. 97 (E.D. Pa. 1996); *Restuccia v. Burk Technology, Inc.*, No. 95-2125 (Mass. Supr. Ct. 1996).

<sup>57</sup> 18 U.S.C §§ 2510 *et seq.*