

Keeping the Toddler out of the Cookie Jar: An Overview of Internet Website and Communications Privacy Issues

November 2000

Table of Contents

Introduction	1
The Federal Trade Commission: Regulating Website Privacy As a Federal “Unfair or Deceptive Practices” Issue	3
FTC Rules and Guidelines for Privacy on the Web	3
FTC Key Elements for Web-Based Privacy: Consumer Choice, Notice, Security, and Access	4
<i>Notice</i>	4
<i>Choice</i>	5
<i>Security</i>	5
<i>Access</i>	5
Children's Online Privacy Protection Act	5
Online Profiling	7
Mobile Internet	8
FTC Enforcement Actions: Privacy and Deceptive Practices	8
The EU–U.S. Data Accord: Privacy and International E-Commerce	11
<i>Notice</i>	12
<i>Choice</i>	12
<i>Onward Transfer</i>	12
<i>Security</i>	12
<i>Data Integrity</i>	12
<i>Access</i>	12
<i>Enforcement</i>	12
The Federal Communications Act: Regulating Privacy Practices of the Provider Getting You to the Internet.	13
Telecommunications Carriers and Consumer Privacy	13
Cable Operators and Consumer Privacy	17
<i>Notice</i>	17
<i>Consent</i>	18
<i>Enforcement</i>	18

State Efforts to Protect Online Consumer Privacy:	
Is a “Patchwork” Approach Imminent?	19
Current State Statutes on Internet Privacy:	
Maryland, Nevada, and Virginia	20
State Bills Targeted at ISPs	21
State Bills Targeted at Websites	23
State Bills Targeted at Entities Holding Personal Information	24
State Bills That Allude to Internet Privacy in General Privacy Bills	25
State Commissions Studying Privacy Issues	26
Federal Legislation: Upcoming Nationwide Privacy Laws.	26
Consumer Internet Privacy Enhancement Act	27
Online Privacy Protection Act of 1999	27
Consumer Privacy Protection Act	28
Conclusion	29



Keeping the Toddler out of the Cookie Jar: An Overview of Internet Website and Communications Privacy Issues

November 2000

Introduction¹

For the Internet, as with any “toddler,” the shift from infancy to the next developmental stage expands possibilities and poses new challenges. The Internet's widening reach certainly promises broad new societal benefits, especially in commerce, education, entertainment, and government. At the same time, the emerging Internet can promote activity that may be troublesome and especially difficult to control, such as its snooping proclivities. Increasingly, we are finding the toddler Internet caught with its hand in the cookie jar.²

¹ Special acknowledgement and appreciation should be given to Rachael V. Abramson and Amy C. McMenamain for their enormous efforts and assistance in preparing this White Paper.

² “Cookies” are small files stored in a user's computer and sent from a website, which enable the website to track a user's online activity.

Consumers consistently express concern about technology and its implications for personal privacy, with numerous studies underscoring the issue. Privacy advocates and others urge that the Internet requires clear and strong parental direction regarding the use of personal identifying information. Today, however, there is no federal statute that squarely regulates how the websites that drive the commercial online world may collect and use the personal information of Internet end users. Moreover, as the reach and use of traditional communications technologies evolve and new broadband flavors are added, there is a growing awareness that consumers' privacy rights can be affected depending upon the technology and service used to access the Internet, and that the rules differ among services.

At the national level, the Federal Trade Commission (FTC) has jumped into issues of consumer privacy, although the absence of a comprehensive national privacy statute has limited the FTC to pursuing website violations in cases of fraudulent or deceptive marketing tactics.³ At the same time, the Federal Communications Commission (FCC) oversees the communications services used to access the Internet and arguably shoulders the responsibility of protecting and ensuring consumer privacy in that regard. In contrast to the FCC's stated policy of a "regulation-free Internet," the FTC has brought over a hundred enforcement actions for online violations and has proposed that Congress enact federal privacy laws, urging that attempts at self-regulation have been ineffective. The status of emerging services, such as location-based wireless Internet services, and the forum that should oversee them, remains to be seen.

At the same time, state legislatures are scrambling to provide some protections for the online privacy of their residents, proposing numerous legislative solutions in bodies throughout the nation. At least 16 state legislatures have introduced variations of an Internet privacy bill in the last year or so. To date, only one state, **Nevada**, has adopted a state Internet privacy law regulating the websites of commercial entities. Some urge that unless we have a federal law, these state efforts will create a web-crippling, crazy quilt of legal standards.

This White Paper provides an overview of governmental responses to the privacy issues implicated by the providers of the online world. Given the breadth of privacy issues and interests, the overview is limited only to the laws and regulations applicable to entities collecting information from consumers or subscribers either through a commercial website or in conjunction with the provision of a telecommunications service. This White Paper does not undertake to review other equally important areas of privacy law, such as laws regulating the disclosure of particular types of content (e.g., financial records or medical records) or laws generally governing the interception of

³ The FTC lacks the general authority to require companies to adopt privacy policies, except as a solution to redress violations in settlement cases. See **Privacy Online: Fair Information Practices in the Electronic Marketplace**, A Report to Congress, Federal Trade Commission, May 2000 ("FTC's May 2000 Report to Congress").

electronic communications (e.g., Communications Assistance to Law Enforcement or the Electronic Communications Privacy Act).

The first section describes the role of the FTC as it addresses consumer privacy issues involving the collection and use of personal information obtained via an Internet session. In addition to the FTC's web privacy rules and guidelines, recent enforcement actions and the European Union/United States Data Privacy Accord are discussed. The second section examines the FCC and its role in regulating the privacy practices of the entities that connect consumers to the Internet, whether traditional dial-up wireline carriers, wireless carriers, DSL providers, cable operators, or others. The third section delineates state endeavors to protect online consumer efforts and offers a sampling of the myriad approaches. The fourth section reviews federal legislative efforts, which will likely form the basis for any national legislation when Congress again turns its attention to privacy. Finally, the White Paper offers a brief conclusion, suggesting swift and certain action to ensure the continued growth of the Internet—action to let the toddler's growth continue to the public's benefit.

The Federal Trade Commission: Regulating Website Privacy As a Federal “Unfair or Deceptive Practices” Issue

FTC Rules and Guidelines for Privacy on the Web

The FTC's current authority to rein in website privacy violations stems from the Federal Trade Commission Act's prohibition of “unfair or deceptive acts or practices in or affecting commerce.”⁴ The act governs advertising, marketing, and sales of products or services without regard to the medium of dissemination. Thus, the FTC's jurisdiction includes such media as print, television, telephone, and radio. Beginning in 1994, the FTC weighed into the Internet media through its first action to stop deception online.⁵

In general, the FTC currently focuses on targeting websites that violate their site's stated privacy policy. The FTC gleans general authority from its **consumer protection laws** applicable to commercial activities.⁶ Absent a specific federal privacy statute, websites can legally collect, use, and disclose personal information gathered about users who visit their site. The FTC can only limit website's practices regarding personal information to the degree

⁴ 15 U.S.C. § 45(a), § 57(a).

⁵ See Federal Trade Commission Staff, Dot Com Disclosures Federal Trade Commission, May 3, 2000, (“FTC Dot Com Paper”).

⁶ See *id.* at 1.

that the website's practices conflict with its stated privacy policy. For example, a likely candidate for FTC action would be a website that attests in a privacy statement to users that it will not disclose a user's personal information and then the website acts deceptively when it sells or discloses that personal information. Faced with deceptive behavior, but without a specific federal privacy law, the FTC enforces the website's stated promises.

Even in the absence of specific federal online privacy laws, however, the FTC has taken an active role to delineate privacy standards and to enforce privacy expectations online. The FTC, for example, has enunciated a set of substantive privacy standards in its *May 2000 Report to Congress*⁷ and in promulgating federal rules to implement the Children's Online Privacy Protection Act. Enforcement actions and industry monitoring have further defined the FTC's visible role in online commerce. With the new U.S./EU Data Accord, the FTC will continue in its role as the primary federal regulator of online privacy in the United States. The FTC's actions to date provide much insight for the future direction of federal privacy regulation.

FTC Key Elements for Web-Based Privacy: Consumer Choice, Notice, Security, and Access

In a *May 2000 Report to Congress*, the FTC recommended pro-consumer federal legislation to protect more adequately privacy online, abandoning its earlier position favoring industry self-regulation. In a three-to-two vote, the FTC proposed to Congress that it should expand the FTC's statutory authority by providing FTC control over websites' use of information.⁸ The FTC also advocated website disclosures involving notice, choice, access, and security to prevent consumer deception.⁹ These elements, particularly notice and choice, resonate in every government action to protect personal information privacy.

Notice

A website should provide customers with "clear and conspicuous" online notice, similar to that of traditional media, disclosing in a specific privacy policy how the site will use the personal information it collects.¹⁰ In May 2000, the FTC issued a 20-page staff working paper detailing ideal scroll

⁷ *Privacy Online: Fair Information Practices In the Electronic Marketplace, A Report to Congress*, Federal Trade Commission, May 2000 ("FTC May 2000 Report to Congress").

⁸ *Id.* See also *Final Report of the FTC Advisory Committee on Online Access and Security*, May 15, 2000 ("Advisory Committee Report"). This Report recommends that each website maintain a security program for the personal data that it holds and that the security program should be appropriate for the circumstances.

⁹ *Id.*

¹⁰ See FTC, *May 2000 Report to Congress* at iii, 15. See also Jeffery D. Knowles & Gary D. Hailey, *Clear and Conspicuous Danger: FTC Disclosure Rules Are An Awkward Fit For Internet Marketers*, Response TV, March 1, 1999.

methods, color contrasts, and mouse clicks to achieve "clear and conspicuous" online disclosure.¹¹

Choice

Users are provided with an option to prevent a website from using their personal information. Notably, this element raises a key, disputed issue of whether users should "opt in" or "opt out" of this choice option. An opt-in approach to this issue would require the consumer to give the website affirmative approval before the website could use the consumer's personal information. An opt-out approach presumes customer approval, permitting websites to use information until the consumer affirmatively asks the website to desist. Some companies support an opt-out approach, and a majority of companies oppose the stringency of the opt-in approach. Although the FTC's *May 2000 Report to Congress* states that 88% of consumers surveyed prefer an opt-in approach, the FTC itself fails to pass judgment or raise the issue, contrary to the detailed discussion in its *1998 Report to Congress*.¹² As discussed in more detail below, however, the FTC seemingly supported the opt-in approach in a recent settlement with online pharmacies.¹³

Security

Websites must take reasonable steps to keep personal information secure and assure accuracy.¹⁴ The FTC's *May 2000 Report to Congress* does not identify a degree of security, only that it must be "appropriate to the circumstances."¹⁵ Additionally, the FTC noted the importance of a website statement as to security practices, but warned against providing too many details that could aid hackers.¹⁶

Access

A user should have access to review, correct, or delete the information collected about the user.¹⁷

Children's Online Privacy Protection Act

Many of these four-prong principles are also embodied in the **Children's Online Privacy Protection Act (COPPA)**, which took effect on April 21,

¹¹ See FTC Dot Com Paper *supra*.

¹² See also FTC's May 2000 Report to Congress at 16 and **Privacy Online: A Report to Congress**, Federal Trade Commission, June 1998 ("FTC's June 1998 Report to Congress").

¹³ See FTC News Release, *Online Pharmacies Settle FTC Charges* (July 12, 2000) <<http://www.ftc.gov/opa/2000/07/iog.htm>>.

¹⁴ See also FTC's May 2000 Report to Congress at 4.

¹⁵ See *id.* at 4, 32.

¹⁶ See *id.* at 19, 33.

¹⁷ The **FTC Advisory Committee Report** (at 2–20) details many of the operational and definitional issues that arise with consumer access to personal information files held by a commercial entity.

2000, to regulate websites' online collection of information obtained from minors.¹⁸ Websites with actual knowledge that they are collecting information from children under the age of 13 must post a **notice** identifying what information the site collects and must obtain prior **verifiable parental consent**.¹⁹ COPPA specifically prohibits websites from conditioning a child's participation in a game or prize offering on the disclosure of more personal information than is necessary to participate.²⁰

Under COPPA, a website's **privacy notice** must describe the information collected by the site and describe how the website uses and discloses that information.²¹ Upon parental request, a website is required to provide a description of the specific types of personal information collected about the child of the parent and must provide the opportunity to prevent the website from further collection of information about that child at any time.²²

A website must reasonably pursue **verifiable parental consent**, including any effort to ensure a parent is notified and gives authorization, before information is collected from the child.²³ When a parent refuses to consent, a website can terminate service provided to a child.²⁴ Consent of the parent is not required, however, when the website collects information used solely to obtain parental consent, when the information is not used to recontact the child, and when the information is not maintained in retrievable form. Also, no parental consent is required to respond to a child's specific request, if the FTC deems the instance appropriate.²⁵ Disclosure of a child's personal information is also permitted to protect a child's safety and for website security, liability, or judicial process.²⁶

FTC rules implementing COPPA went into effect on April 21, 2000.²⁷ These rules require an owner of a website (or online service, chatroom, etc. directed to children) with actual knowledge that it collects information from children to post a "clear and prominent" link to a "clear and understandable" privacy notice on the website's homepage, and in close proximity to a request for personal information on any other page. The notice must include a description of the type of information collected and the name, address, telephone number, and email address of those collecting information.²⁸ The rules also identify methods for websites to obtain "verifiable parental con-

¹⁸ See Children's Online Privacy Protection Act § 1303b(1), 15 U.S.C. §§ 6501 *et. seq.* (1998).

¹⁹ See *id.* at § 1303(a)(1), (b)(1)(A)(i), (ii).

²⁰ See *id.* at § 1303(b)(1)(C).

²¹ See *id.* at § 1303(b)(1)(a)(i).

²² See *id.* at § 1303(b)(1)(B).

²³ See *id.* at § 1302(9).

²⁴ See *id.* at § 1303(b)(1)(a)(i).

²⁵ See *id.* at § 1303(b)(2)(A), (B), (C).

²⁶ See *id.* at § 1303(b)(2)(D), (E).

²⁷ See 16 C.F.R. § 312.4(a), (b) (1999).

²⁸ See *id.* at § 312.4(b)(2).

sent” before collecting information from a child. Thus, with certain exceptions, COPPA clearly mandates an opt-in approach for young children as the protected class. Parental consent is required unless the website uses information and deletes it after responding to a child's one-time request.²⁹ A parent can revoke consent or review information collected.³⁰ FTC review of websites' self-regulatory guidelines or participation in an Internet privacy seal program, such as TRUSTe, Better Business Bureau Online, CPA WebTrust, or the Entertainment Software Ratings Board, can provide websites with a “safe harbor,” or presumed compliance, with COPPA.³¹

In a step toward enforcing the COPPA rules, the FTC last July sent scores of emails to children's websites directing them to comply with the COPPA and the FTC's implementing rules. The FTC reported that approximately half of the sites collecting children's personally identifiable information had COPPA compliance problems, based on a recent Internet review. The FTC cautioned those websites that they would be monitored and could be subject to Commission review for further legal action.³²

Online Profiling

Two recent FTC reports have highlighted the agency's growing concerns with the issue of **online profiling**. In its two-part *Online Profiling: A Report to Congress* issued in June and July 2000,³³ the FTC described the nature of online profiling and its potential effects on consumer privacy. The FTC focused specifically on the practices of network advertising companies that insert banner ads onto a commercial website and then collect certain information on the Internet habits of users of the website, sometimes without the knowledge of the website host. Banner ad companies may then combine this online information with other offline personal information about the user's buying habits to create a separate personal information profile. To address the FTC's concerns, the leading Internet network advertisers formed the Network Advertising Initiative (NAI) principles for fair information practices. In essence, the NAI members have agreed to require by contract that all of its website hosts include “robust” notice and opt-out choice on the issue of profiling. While the FTC agreed with the industry's position, the agency also urged Congress to pass legislation to better protect consumers from all unwanted online profiling, noting that the NAI represented 90%, but not 100%, of the network advertising industry.

²⁹ See *id.* at § 312.5(c), (b)(2).

³⁰ See *id.* at § 312.6(a)(2), (3).

³¹ See *id.* at § 312.10(a), (b)(4), (c).

³² See FTC News Release, *Web Sites Warned to Comply With Children's Online Privacy Law: FTC Also Works to Educate Children's Sites About Law's Privacy Protections*, July 17, 2000.

³³ See *Online Profiling: A Report to Congress*, Federal Trade Commission, June 2000, and, *Online Profiling: A Report to Congress*, Federal Trade Commission, July 2000.

Mobile Internet

Finally, the FTC has expressed at least a preliminary interest in the protection of **privacy of mobile users connecting to the Internet**. On December 11 and 12, 2000, the FTC will hold workshops to discuss issues related to “emerging wireless Internet and data technologies and the privacy, security, and consumer protection issues they raise.”³⁴ At this time, the FTC has not articulated how it would apply its privacy principles or enforcement actions to mobile and wireless providers of Internet services.

FTC Enforcement Actions: Privacy and Deceptive Practices

Since 1994, the FTC has brought more than a hundred actions against online companies for deceptive practices, including four privacy-related enforcement actions.³⁵ Through enforcement actions against often larger sites, the FTC is regulating Internet privacy by example. The FTC has settled all cases thus far by requiring that a website post a privacy policy. In one recent settlement, however, the FTC applied the hotly contested opt-in approach, prohibiting a website from “selling, renting, leasing, transferring, or disclosing” personal information without user's consent.³⁶

As noted, the FTC's primary enforcement actions are pursuant to its statutory obligations regarding fraudulent or deceptive commercial practices, generally against a website that misrepresents itself, deceives its users, or disregards its own or another site's privacy policy and discloses personal information. For example, on July 10, 2000 the FTC brought an enforcement action against **Toysmart.com**, which advertised the sale of its user's personal information as an asset in its bankruptcy proceedings despite the company's public attestation that it would “never” share information with a third party.³⁷ The FTC settled the case later the same month by allowing Toysmart, whose largest owner is Disney, to sell its customer data only if the buyer promises to uphold Toysmart's privacy pledge and requiring that any change made by a successor to the original privacy policy must be approved by customers on an opt-in basis. The bankruptcy court must approve the FTC-Toysmart settlement; approximately 40 State Attorney Generals have objected to the FTC settlement as too lenient, and asked the bankruptcy court for further consumer protections.³⁸

³⁴ FTC News Release, *Mobile Wireless Web, Data Services, and Beyond: Emerging Technologies and Consumer Issues*, November 14, 2000.

³⁵ See FTC Dot Com Paper. For a list of FTC Privacy Initiatives go to <http://www.ftc.gov/privacy/index.html>.

³⁶ See FTC News Release, *Online Pharmacies Settle FTC Charges*, July 12, 2000 (<<http://www.ftc.gov/opa/2000/07/iog.htm> >).

³⁷ See FTC News Release, *FTC Sues Failed Website, Toysmart.com, for Deceptively Offering for Sale Personal Information of Website Visitors*, July 10, 2000 (<<http://www.ftc.gov/opa/2000/07/toysmart.htm>>); *FTC v. Toysmart.com, LLC, and Toysmart.com, Inc.* (District of Massachusetts) (Civil Action No. 00-11341-RGS).

The Toysmart litigation was also the FTC's first and only COPPA enforcement action.³⁹ Toysmart collected detailed personal information about its visitors, including minors, and attempted to sell the information as an asset in its bankruptcy proceedings. The FTC filed a complaint in district court that the site's collection violated COPPA and the sale was an unfair trade practice.⁴⁰ FTC action apparently deterred higher bids for this information. Toysmart took this asset off the auction block when Disney, the highest bidder and Toysmart's majority owner, only offered \$50,000.⁴¹ The FTC director of the Bureau of Consumer Protection noted that this first charge against Toysmart "is only the start of our efforts" to enforce COPPA.⁴²

On July 6, 2000, the FTC settled privacy claims against **Internet pharmacies** that misrepresented security and encryption measures. Although the websites had not actually transferred any information to third parties, the FTC settlement prohibits the websites from disclosure of information without prior consumer consent (opt in) and requires each of the websites to post a privacy policy.⁴³ Significantly, this settlement raises the controversial political question whether the FTC supports the requirement of customer opt-in procedures and whether the FTC would apply opt-in standards.

From 1998–2000 the FTC also settled online privacy cases against three other online companies—GeoCities, Young Investor, and ReverseAuction.com Inc. In **GeoCities**, third parties had solicited website members after the website assured members that the optional information they provided (including members' email address) would not be disclosed.⁴⁴ In **Young Investor**, the website owned by Liberty Financial Companies used information to identify individuals from answers given to contest eligibility forms that the website represented as "totally anonymous."⁴⁵ In **ReverseAuction**,

³⁸ See Stephanie Stoughton, *States Weigh In On Toysmart Privacy Case, 38 Attorneys General Join Opposition To Sale Of Data*, The Boston Globe, July 26, 2000. At this time, the bankruptcy proceedings are still pending.

³⁹ See *FTC v. Toysmart.com, LLC, and Toysmart.com, Inc.* (District of Massachusetts) (Civil Action No. 00-11341-RGS, 2000). See also FTC News Release, *FTC Announces Settlement With Bankrupt Website, Toysmart.com, Regarding Alleged Privacy Policy Violations*, July 21, 2000.

⁴⁰ See Justin Pope, *Toysmart Wants Better Offer For Customer List*, The Associated Press, July 27, 2000. See also Stephanie Stoughton, *Judge Disputes FTC Settlement On Web Store Database*, The Boston Globe, July 27, 2000. COPPA went into effect April 21, 2000 and Toysmart's dinosaur trivia contest directed at children that amounted to the violations ran from May 1 until May 22, 2000.

⁴¹ See Justin Pope, *Toysmart Wants Better Offer For Customer List*, The Associated Press, July 27, 2000. See also Stephanie Stoughton, *Judge Disputes FTC Settlement On Web Store Database*, The Boston Globe, July 27, 2000. At this time, the bankruptcy case is still pending.

⁴² See FTC News Release, *FTC Announces Settlement With Bankrupt Website, Toysmart.com, Regarding Alleged Privacy Policy Violations*, July 21, 2000.

⁴³ See FTC News Release, *Online Pharmacies Settle FTC Charges*, July 12, 2000 (<<http://www.ftc.gov/opa/2000/07/iog.htm>>).

⁴⁴ See FTC News Release, *Internet Site Agrees to Settle FTC Charges of Deceptively Collecting Personal Information in Agency's First Internet Privacy Case*, Aug. 13, 1998 (<<http://www.ftc.gov/opa/1998/9808/geocitie.htm>>). See also CNET NEWS.Com, *FTC, GeoCities Settle on Privacy*, August 13, 1998 (<<http://news.cnet.com/news/0-1005-200-332199.html>>).

the auction site registered with its competitor eBay to collect eBay users' email addresses to spam eBay members with deceptive and unfair ReverseAuction site promotions and thereby violated eBay's privacy policy.⁴⁶ In all three cases, the FTC settled the case after each company agreed to post a privacy policy. In addition, under the settlement, GeoCities and Young Investor have agreed to obtain prior parental consent before the sites collect personal information from children. Privacy advocates called the settlement with ReverseAuction a "slap on the wrist." The chairman of the Senate Commerce Communications Subcommittee reflected on government action versus industry self-regulation noting, "the difference between posting a privacy policy and actually providing privacy to users is huge."⁴⁷

In addition to formal enforcement actions, the FTC's monitoring and informal warnings also keep the agency, and industry, aware of potential online privacy issues. The FTC's Bureau of Consumer Protection began conducting "Surf Days" in 1996 to detect Internet fraud and deception.⁴⁸ Surf Days can involve the efforts of FTC attorneys and investigators, the Securities and Exchange Commission, the U.S. Postal Inspection Service, the Federal Communications Commission, and state and local law enforcement officials. Past Surf Days have included nationwide and international task forces. Sometimes, FTC informal warnings have been effective: the FTC estimates that 20 to 70 percent of those websites warned comply with the law within a month.⁴⁹ Also, the FTC continues to investigate consumer complaints. The FTC's Consumer Response Center averages 40,000 calls a month assisting consumers and businesses that contact the toll free helplines (877-FTC-HELP and 877-ID-THEFT). The FTC also has an online complaint form on its website.⁵⁰

⁴⁵ See FTC News Release, *Young Investor Website Settles FTC Charges*, May 6, 1999 (<<http://www.ftc.gov/opa/1999/9905/younginvestor.htm>>). See also *Liberty Financial Companies, Inc.*, No. C-3891 (FTC August 12, 1999).

⁴⁶ See FTC News Release, *Online Auction Site Settles FTC Privacy Charge*, January 6, 2000 (<<http://www.ftc.gov/opa/2000/01/reverse4.htm>>); See also *FTC v. Reverse Auction.com, Inc.*, No. 00-0032 (D.D.C. January 6, 2000).

⁴⁷ FTC Airs Online Privacy Concerns About "Cookies," Databases, TR Daily, June 13, 2000. See also Greg Snadovol & Troy Wolverton, CNET NEWS.com, Security, Privacy Issues Make Net Users Uneasy, January 7, 2000.

⁴⁸ See FTC Chairman Robert Pitofsky, *Internet Fraud*, Address before the Subcommittee on Investigations of the Senate Governmental Affairs Committee, Feb. 10, 1998.

⁴⁹ See FTC General Counsel Debra A. Valentine, *Cross-Border Canada/U.S. Cooperation in Investigations and Enforcement Actions*, Address to Canada/U.S. Law Institute Case Western Reserve University School of Law, April 15, 2000.

⁵⁰ See FTC Director of Bureau of Consumer Protection Jodie Bernstein, *Online Privacy: Recent Commission Initiatives*, Address to the Subcommittee on Courts and Intellectual Property in the House Committee on the Judiciary, May 18, 2000.

The EU–U.S. Data Accord: Privacy and International E-Commerce

While the United States has chosen a market-driven model for the growing Internet economy, Europe has endorsed a government-managed model and has become wary of the U.S. self-regulatory approach to Internet privacy protections. Without a United States and European Union (EU) agreement, Europe's potentially sweeping privacy laws would cripple U.S.–EU trade, which reaches \$120 billion annually.⁵¹ After nearly two years of negotiations, the United States and the EU reached a "Safe Harbor" Data Privacy Accord in March 2000.⁵² The European Commission endorsed the Accord in July 2000, despite last minute concerns of the European Parliament, and the Accord is now binding on 15 EU member states.⁵³ The safe harbor principles were published in the *Federal Register* in July 2000 and are currently in place.⁵⁴

Under the Accord, a U.S. or European company engaged in web-based commerce may voluntarily commit to adhere to a set of privacy rules governing commercial and information transactions over the Internet. In return for this commitment, the company is granted a "safe harbor" from litigation or prosecution in Europe. The "safe harbor" provides a U.S.-based company with the presumption that they have an "adequate" standard of privacy under EU law. The names of U.S.-based companies qualifying for the "safe harbor" are retained on a list kept by the U.S. Department of Commerce for European perusal of possible business partners. To be listed, a U.S. company may either voluntarily self-certify publicly to the Department of Commerce that it meets the "adequacy" standard, or it may join an adherent self-regulatory privacy program. For annual self-certification, the company should send a signed letter to the Department of Commerce describing its privacy policy and recourse mechanisms, among other disclosures, all of which will be pub-

⁵¹ The EU enacted the Directive on Data Protection, privacy legislation for its member countries, which became effective October 25, 1998. In practice, the act would prohibit EU states from trading to non-member states that do not have equivalent standards of data protection. The EU directive requires an "adequate" level of privacy protection. See Safe Harbor Privacy Principles, U.S. Department of Commerce (July 21, 2000) (<<http://www.ita.doc.gov/td/ecom/shprinciplesfinal.htm>>). See also White House News Release, *Fact Sheet: Data Privacy Accord With EU (Safe Harbor)*, May 31, 2000.

⁵² U.S., *EU Conclude Negotiations for Data Privacy "Safe Harbor"*; TR Daily, March 14, 2000.

⁵³ See Warren's Washington Internet Daily at 5 (July 14, 2000). See also *EU Commission Endorses Data Privacy Pact With U.S.*, Reuters, July 27, 2000. See Mary Greczyn & Sasha Samberg, *EC Unveils Proposals to Streamline Rules and Provide Access*, Communications Daily, July 13, 2000. See also *European Commission OKs U.S. "Safe Harbor" Data Privacy*, TR Daily, July 27, 2000. The European Parliament voted to reject the safe harbor agreement but the European Commission approved the Safe Harbor decision over the European Parliament's opposition. The European Commission did state, however, that they would re-open negotiations with the U.S. next year if the concerns of the Parliament prove to be "well founded."

⁵⁴ See Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 142 (2000). See Letter from Robert S. LaRussa, Acting Under Secretary for International Trade Administration, U.S. Department of Commerce, to U.S. organizations 1 (July 21, 2000).

licly available.⁵⁵ A company must continue to adhere to the principles even after the company no longer is listed if the company still uses data collected while it was listed.⁵⁶ The “safe harbor” principles are:⁵⁷

Notice

Before the organization uses collected information, an organization must provide clear and conspicuous notice including the purpose of collection, contact information, types of third parties who will use the information, and the consumer's choices to limit information use.

Choice

A customer must have the ability to “opt out” of a company's routine data collection. In cases of sensitive information (such as medical, sex, race, ethnicity, or political and religious beliefs), a company must first obtain opt-in approval from the customer.

Onward Transfer

Any third party that the information is transferred to must also abide by the “safe harbor” principles.

Security

A company must take reasonable precautions to avoid information disclosure or misuse.

Data Integrity

A company cannot use personal information for purposes other than those stated.

Access

Companies must provide customers with access to change or delete their personal information.

Enforcement

Companies must have mechanisms in place to assure compliance, including recourse and consequences for noncompliance.

Under the Accord, an enforcement action against a company for an alleged privacy violation would involve a three-stage process.⁵⁸ First, a com-

⁵⁵ See Department of Commerce, Frequently Asked Questions: Self-Certification (July 21, 2000) (<<http://www.ita.doc.gov/td/ecom/FAQ6SelfCertFINAL.htm>>).

⁵⁶ See *id.*

⁵⁷ See Safe Harbor Privacy Principles, U.S. Department of Commerce, July 21, 2000 (<<http://www.ita.doc.gov/td/ecom/shprinciplesfinal.htm>>).

⁵⁸ See How Will the “Safe Harbor” Arrangement For Personal Data Transfers To The US Work?, European Union (visited July 31, 2000) (<http://wuropea.eu.int/comm/internal_market/en/media/dataprot/news/datatransf.htm>).

pany may use alternative dispute resolution to resolve complaints privately. If websites fail to comply with these rulings, the **Federal Trade Commission** (or, for cases involving airlines, the Department of Transportation) may bring an enforcement action. If a “safe harbor” company is found to have violated the “safe harbor” principles, the FTC may find that it is liable for misrepresentation or deceptive trade practice, and face heavy fines. Further noncompliance can result in a company's removal from the Department of Commerce's “safe harbor” list, which would presumably cause difficulty for any company engaging in e-commerce in Europe.

The Federal Communications Act: Regulating Privacy Practices of the Provider Getting You to the Internet

While the FTC has directed its efforts at website privacy, two provisions of the Federal Communications Act, Sections 222 and 631, provide privacy protections for consumers' use of the transmission services to and from the Internet, i.e., the telecommunications and cable networks.⁵⁹ Notably, however, these provisions do not regulate the privacy practices of Internet service providers, websites, or electronic commerce. Rather, the privacy protections of the Communications Act concern the companies offering consumers the transmission lines and services over which the Internet and electronic commerce ride. Equally significant is the fact that the level of statutory privacy protection under the law is quite different, depending on whether the consumer chooses a cable operator's service or a telecommunications carrier's service.

Telecommunications Carriers and Consumer Privacy

Section 222 of the Communications Act, 47 U.S.C. § 222, governs the privacy practices of carriers offering telecommunications services, such as incumbent local telephone companies, long-distance providers, and mobile service (cellular and PCS) providers.⁶⁰ This section also encompasses broadband services such as DSL. Specifically, the carrier is restricted in its use and disclosure of Customer Proprietary Network Information (CPNI), including such information as the services ordered by the customer, the telephone numbers called and length of the calls, and the customer's telephone bill.⁶¹ Under Section 222, a carrier is prohibited from using, disclosing, or permit-

⁵⁹ 47 U.S.C. §§ 222, 551.

⁶⁰ See Communications Act of 1934, 47 U.S.C. § 222 (1999).

⁶¹ See *id.* at § 222(e)(1)(1)(A).

ting access to CPNI unless it has the customer's consent. The law balances this proscription, however, with several exceptions permitting the use and disclosure of CPNI under certain circumstances. For example, a carrier may use or disclose CPNI to engage in billing functions, to protect against a user's unlawful acts, or for telemarketing purposes when the customer has initiated the call.⁶² A carrier may also disclose CPNI to third parties for limited purposes, such as to publish telephone directories, disclosures made at the customer's written request, or to provision the services requested by the customer.⁶³ The CPNI restrictions are also limited because they do not apply to aggregate customer information, which a carrier can provide to other carriers or persons on a reasonable and nondiscriminatory basis.⁶⁴

In addition to the statutory protections, the FCC has also engaged in significant rulemaking proceedings implementing the privacy protections of Section 222; these rules, however, have been declared **unconstitutional** by one federal appeals court, largely because of the perceived conflict between the FCC's opt-in approach to consumer consent and the First Amendment rights of carriers to speak with customers. Beginning in 1998, and at the request of some carriers, the FCC's **Second Report and Order** first defined the scope and meaning of the carrier's Section 222 obligations.⁶⁵ The FCC specifically authorized carriers to use CPNI to market offerings within the carrier's existing relationship with its customer.⁶⁶ Significantly, the FCC also adopted a strong opt-in approach, requiring carriers to obtain customer approval *before* using CPNI in a manner beyond the existing customer-carrier relationship.⁶⁷ Thus, for example, under the FCC's rules, the carrier would be required to obtain the customer's prior consent if the carrier wanted to use the customer's local telephone calling information to market another service to the customer such as long distance telephone service. Additionally, the FCC's rules required carriers to provide customers with notice of their CPNI rights before soliciting a customer's opt-in approval.⁶⁸

On reconsideration of the *Second Report and Order*, the FCC's subsequent orders scaled back the severity of the opt-in approach on carriers. In general, the FCC reacted to the industry's complaints that its privacy rules interfered

⁶² See *id.* at § 222(d).

⁶³ See *id.* at § 222(c)(1), (c)(2), (e).

⁶⁴ See *id.* at § 222(c)(3).

⁶⁵ See *In the Matter of Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-155, **Second Report and Order and Further Notice of Proposed Rulemaking**, at ¶¶ 1, 3, 7 (rel. Feb. 26, 1998) ("Second R&O"). See *In the Matter of Implementation of the Telecommunications Act*, CC Docket No. 96-115, **First Report and Order** (August 7, 1996) (pertaining to alarm monitoring services records of the occurrence of calls they received, a type of CPNI). Significantly, Section 222 does not provide the FCC with express authority to promulgate CPNI rules. See 47 U.S.C. § 222.

⁶⁶ See *id.* at ¶ 4(a).

⁶⁷ See *id.* at ¶ 4(b). See also *U.S. West v. FCC*, 182 F.3d 1224, 1229, 1230 (10th Cir. 1999).

⁶⁸ See *Second Report and Order* at ¶ 4(b).

excessively with the carrier-customer relationship and also to the premise that CPNI should reinforce the user's reasonable privacy expectations. In May 1998, for example, the FCC issued a **CPNI Clarification Order** noting that "independently derived information" regarding customer premises equipment and information services was not CPNI, and such information could be used for carriers' marketing purposes. The order also clarified that a customer's name, address, and telephone number, if published, were "subscriber list information" and not subject to the statutory CPNI protections.⁶⁹ Further, the FCC also developed exceptions to its restrictive opt-in approach in an **Order on Reconsideration and Third Report and Order**,⁷⁰ where the FCC refined the terms by which a carrier could use CPNI without customer approval under the "customer-carrier relationship."⁷¹ Specifically, the FCC allowed wireline carriers to use CPNI to market some (but not all) information services and customer premises equipment without first gaining the customer's approval.⁷² Wireless carriers were provided even more flexibility to use CPNI in the marketing of wireless CPE and information services. The FCC further permitted carriers to use CPNI to "win back" those customers who had switched to competitors.⁷³ The FCC also amended the strict and costly disclosure requirements of the *Second Report and Order* by freeing carriers from record keeping constraints, leaving the details of compliance to the carriers.⁷⁴

In August 1999, during the time that the FCC was addressing additional industry concerns regarding CPNI, the **Tenth Circuit** vacated the *Second Report and Order* as an unconstitutional infringement on the carrier's right to commercial free speech. On review of the FCC's order, the Tenth Circuit held that the FCC's regulations violated the First Amendment because the FCC failed to consider the opt-out approach to obtaining customer approval, a less restrictive alternative than the FCC's opt-in mandate. This, the court reasoned, meant that the CPNI regulations were not narrowly tailored to

⁶⁹ See *In the Matter of Implementation of the Telecommunications Act of 1996, Order on Reconsideration*, CC Docket No. 96-115, ¶ 8 (Sept. 3, 1999) ("**Order on Reconsideration**"). See also *In the Matter of Implementation of the Telecommunications Act of 1996, Clarification Order*, CC Docket No. 96-115, ¶ 8. See also 47 U.S.C. § 222(f).

⁷⁰ *In the Matters of Implementation of the Telecommunications Act of 1996, Third Report and Order, the Second Order on Reconsideration of the Second Report and Order, and Notice of Proposed Rulemaking*, CC Docket No. 96-115 (September 9, 1999) ("**Third Report and Order**").

⁷¹ In the **Third Report and Order**, the FCC developed rules requiring carriers to provide subscriber list information with updates to any requesting directory publisher, in the format the publisher requested, at the baseline reasonable rate of \$.04 per listing, and on the same terms and conditions, thus preventing unfair LEC practices and encouraging competition in directory publishing. See **Third Report and Order** at ¶ 8 (September 9, 1999).

⁷² See *Order on Reconsideration*, ¶ 6(c), 8.

⁷³ See *id.* at ¶ 6(d).

⁷⁴ See *id.* at ¶ 1, 6(f). The FCC adopted the **Order On Reconsideration** Aug. 16, 1999, two days before the Tenth Circuit handed down the decision to vacate the FCC's *Second Report and Order*. See *id.*

meet their statutory objective.⁷⁵ Applying the Supreme Court's Central Hudson⁷⁶ standard of review for commercial speech cases, the Court determined that the FCC impermissibly restricted more speech than was necessary to serve the statutory interests.⁷⁷ In June 2000, the U.S. Supreme Court declined to hear the case on appeal.⁷⁸

As it stands, the **Tenth Circuit decision** is a high hurdle for the FCC to meet. According to the court, the FCC's rules were defective because they were based on an inadequate record and aimed at the wrong interest because competition, and not privacy, is the protected interest embodied in the Telecommunications Act.⁷⁹ The FCC may adopt an opt-in approach, therefore, only if it can demonstrate that it serves the congressional interest of competition in the telecommunications market. Naturally, under this test, the less intrusive opt-out approach may be more appropriate and would certainly require further FCC consideration.

As of yet, however, the FCC has taken no formal remand action.⁸⁰ The FCC may, of course, decide to initiate further proceedings on remand in order to satisfy the Court's concerns and to substantiate or modify the vacated CPNI rules. Because Section 222 of the Act was not under challenge, the statutory privacy protections remain intact and may be enforced in future adjudications. These enforcement actions may arise through a complaint or enforcement action at the FCC or through a complaint in federal district court.⁸¹ It is uncertain whether the FCC's CPNI orders may also be useful as a valid interpretation of Section 222 in such future adjudications.

⁷⁵ See *U.S. West*, 182 F.3d at 1238-39.

⁷⁶ 447 U.S. 557, 561. The **Central Hudson** four-part test permits government regulation of First Amendment speech in the case of: (1) lawful and non-misleading speech; (2) when the government has a "substantial state interest in regulating the speech; (3) the regulation directly and materially advances that interest; and (4) the regulation is no more extensive than necessary to serve the interest."

⁷⁷ See *U.S. West*, 182 F.3d at 1238-39.

⁷⁸ See *U.S. West, Inc.*, 182 F.3d 1224 (certiorari denied by **Competition Policy Institute v. US West, Inc.**, 120 S.Ct. 2215 (June 5, 2000)). The Competition Policy Institute asked the Supreme Court for review because the FCC was content to rewrite the rules to pass the constitutional hurdle rather than appeal. See Heather F. Weaver, *Supreme Court Declines to Review Privacy Rules*, RCR Communications Report 1, June 12, 2000.

⁷⁹ See *id.* at 1235, 1236, 1237 (referencing the preamble to the Telecommunications Act that declares it "[a]n act to promote competition and reduce regulation in order to secure lower prices and higher quality services for American telecommunications consumers and encourage the rapid deployment of new telecommunications technologies.").

⁸⁰ A recent *ex parte* filing by the trade association USTA suggests that the FCC staff intend to proceed with further rulemaking proceedings on remand from the Tenth Circuit decision and/or with enforcement actions. See United States Telecom Association May 18, 2000 *Ex Parte* at 1-2 (FCC staff explained to USTA that if a complaint were filed pursuant to section 208, the FCC would apply its interpretation articulated in the Reconsideration Order. USTA also reported that FCC staff expected to take "expeditious action" to implement a rulemaking proceeding after the Supreme Court's denial of certiorari).

⁸¹ See 47 U.S.C. §§ 207, 208.

In October 1999, amendments to Section 222 of the Communications Act established additional **privacy protections regarding wireless location information** obtained by wireless carriers. These amendments to Section 222 provide that the wireless carrier may not use or disclose wireless call location information unless the wireless customer has provided “express prior authorization.”⁸² These amendments to Section 222 will likely garnish more FCC activity. Currently, as part of its E911 initiatives, the FCC requires commercial wireless carriers to implement technology identifying the location of mobile subscribers. The E911 rules are designed for 911 calls from mobile subscribers to include location coordinates that are sent automatically to emergency assistance personnel. Because the costs to implement such E911 location technology can be quite high, the industry is looking to use subscriber location information for commercial, as well as emergency 911, purposes. While the FCC has yet to interpret the 1999 amendments, they may prove to be at odds with the FCC's other goals for rapid deployment of life-saving 911 location technology.⁸³

Cable Operators and Consumer Privacy

Section 631 of the Communications Act, 47 U.S.C. § 551, establishes a separate set of privacy protections for the customers of cable operators. In several key respects, the privacy rights of cable subscribers are different from, and more extensive than, the consumer privacy protections of Section 222. As described in more detail below, the cable privacy provisions require the cable operator to engage in detailed **notice** filings and **opt-in** consent to disclose personal information.

Notice

At least once a year, cable companies or “other services” using cable operator's facilities must provide clear and conspicuous **notice** to each subscriber detailing the nature, frequency, and use of personally identifiable information (PII) collected about the individual customer and describing the third parties to whom any PII disclosure may be made.⁸⁴ The notice must also state how long the cable operator will retain the information and the subscribers' right to **access** information and enforce limitations on a carrier's disclosure.⁸⁵

⁸² 47 U.S.C. § 222(f).

⁸³ Significantly, on December 11 and 12, 2000, the FTC also intends to hold a series of workshops on privacy issues and commercial mobile services, including the use of subscriber location information. FTC News Release, *The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues*, November 14, 2000.

⁸⁴ See Cable Communications Policy Act of 1984, Pub. L. No. 98-549, § 631(a)(1)(E)(2)(B), (a)(1)(B), 98 Stat. 2780 (1984) (codified as amended at 47 U.S.C. § 551 (1999)).

⁸⁵ See *id.* at § 631(a)(1)(C), (D), (E).

Consent

Generally, a cable provider must obtain a customer's prior written **consent to disclose** and collect PII (opt-in), including viewing habits and transactions, except when disclosure is necessary for a business activity related to a cable or "other service," to detect unauthorized cable communications reception, or as required by a court order.⁸⁶ Disclosure of a subscriber's name and address is excluded from the opt-in requirement, however, if the subscriber has the opportunity to prohibit or limit disclosure (opt-out) and the disclosure does not reveal even indirectly the subscriber's viewing habits or the nature of the subscriber's cable transactions.⁸⁷ Companies are also free to disclose aggregate data, which does not identify individuals personally and is therefore not PII.⁸⁸ Customers must have "reasonable" access to PII and the opportunity to correct errors. The cable operator must also destroy unnecessary PII.⁸⁹

Enforcement

The provisions of Section 631 can impose significant penalties on a cable operator's noncompliance. First, the Section 631 rights are enforced through an action in federal district court, typically a class-action lawsuit, where more pro-plaintiff juries, rather than the FCC, decide the cable operator's culpability. Second, the law establishes significant **monetary penalties** for violating the Section 631 privacy protections, especially in a class-action lawsuit: not less than \$100 per violation for each day of violation, or \$1000, whichever is greater. A court also may award punitive damages.⁹⁰ It is important to note that these severe penalties can be levied in addition to any other lawful remedy available to cable subscriber plaintiffs.⁹¹

It is also significant to note that new **two-way services of cable operators** raise issues of the interplay between Sections 222 and 631 of the Communications Act. For example, some cable operators are also state-certificated competitive local exchange carriers and offer traditional telephone or dedicated line services using their own cable lines and infrastructure as well as the infrastructure of incumbent local exchange carriers. In that context, it is generally acknowledged that cable operators are "telecommunications carriers" when offering telephone service to the public. It follows, therefore, that the privacy protections of Section 222, which are imposed on "every telecommunications carrier," would apply to cable-based telephony services; arguably, it also follows that Section 631 privacy obligations do not apply to cable-based telephony. An issue may also exist regarding the statutory privacy

⁸⁶ See *id.* at § 631(b)(1), (c)(1), (c)(2)(A), (B); § 631(c)(2)(C)(ii).

⁸⁷ See *id.* at § 631(c)(2)(C)(i).

⁸⁸ See *id.* at § 631(a)(2).

⁸⁹ See *id.* at § 631(d), (e).

⁹⁰ See *id.* at § 631 (f)(2)(A), (C).

⁹¹ See *id.* at § 631 (f)(3).

obligations that apply to cable-based high-speed Internet access services. These services generally offer the consumer Internet access (e.g., Roadrunner's service) and the two-way broadband transmission functionality of the cable facilities from the ISP's location to the end user. The FCC, to date, has not defined whether this combined high-speed Internet service or the transmission functionality is to be deemed "telecommunications," or "telecommunications service," nor has it determined whether the cable operator would be a "telecommunications carrier." The FCC has, however, released a **Notice of Inquiry** raising issues of the proper regulatory classification of cable modem service, which also notes the distinct privacy laws that may apply.⁹² Federal courts have suggested differing opinions on this issue, as well.⁹³ The ultimate resolution of these vexing statutory classification issues will also likely bear on what, if any, privacy obligations apply to high-speed, cable-based Internet access service.

State Efforts to Protect Online Consumer Privacy: Is a "Patchwork" Approach Imminent?

Rather than waiting for the federal government to make any upcoming decision on privacy protections, some states have mobilized to fill the void and protect their residents. These efforts, in a few states, have included state legal cases brought by **state attorneys general** under general consumer protection law.

For example, two state attorneys general have sued to protect Internet consumer privacy under unfair or deceptive practices law. In Missouri, the attorney general has taken the view that privacy issues will be prosecuted using current consumer protection laws—the Missouri attorney general sued Internet website **More.com** for misrepresenting to users that the website will not share personal information with third parties.⁹⁴ The Michigan attorney general action against the Internet advertising company, **DoubleClick**, is another recent example of state action to protect consumer privacy.⁹⁵ The state alleged that the company violated its consumer protection laws by creat-

⁹² *In the Matter of Inquiry Concerning High-Speed Access to the Internet Over Cable and Other Facilities*, **Notice of Inquiry**, GN Docket 00-185, FCC 00-355, ¶ 20 (rel. Sept. 28, 2000).

⁹³ See *Gulf Power Co. v. FCC*, 208 F.3d 1263, 1278, 1279 (11th Cir., 2000); *AT&T Corp. v. City of Portland*, 216 F.3d 871 (9th Cir. 2000); *MediaOne Group, Inc. v. County of Henrico*, 97 F.Supp.2d 712 (E.D. Va. 2000).

⁹⁴ "Web site violated law by giving out personal information to third parties after stating it would not, Nixon says," **News** (Sept. 14, 2000), *found at*, www.ago.state.mo.us/091400htm.

⁹⁵ **Press Release**, Michigan Attorney General Jennifer M. Granholm (rel. February 17, 2000).

ing and selling profiles of users' Internet surf habits through implanting of "cookies" in the user's computers without consent.

Perhaps more significant, however, are the number of state legislatures introducing legislative bills that would establish specific statutory consumer privacy protections for Internet and online users. In general, **state legislative bills** address two key elements of privacy protection for consumers: notice and choice. "Notice" requires a website to post a privacy statement or an Internet service provider to send an email to customers notifying them of possible use of their online movements and personal information. It is a preventative measure to educate the consumer of possible privacy abuses. "Choice" evokes the contentious debate between opt-in and opt-out approaches and is arguably the heart of online privacy protection. Most state legislation is aimed at preventing an ISP or website from using collected information without the consumer's opt-in consent. The opt-out approach is taken in less state legislation, which would permit ISPs and websites to presume they have consumer consent until the consumer revokes permission.

The first round of state legislation introduced to target and protect privacy on the Internet began in 1998. Minnesota and California were two of the first drafters of this wave of legislation from which other states have developed their own. Although most of these bills died at the end of last session, it is reasonable to expect many of these bills will be resurrected and reworked with renewed vigor in the next state legislative sessions.

Current State Statutes on Internet Privacy: Maryland, Nevada, and Virginia

The states of Maryland, Nevada, and Virginia have passed Internet privacy protection laws. As explained below, Nevada's law regulates Internet service providers while the laws of Maryland and Virginia are directed at establishing privacy practices on government websites.⁹⁶

Nevada regulates both commercial and governmental providers of Internet services. Nevada Chapter 530 Section 21⁹⁷ includes both notice and consent requirements. The 1999 law generally applies an opt-in approach with an opt-out exception. Providers of Internet service, including those that charge a subscriber for access to Internet or email, must keep all subscriber information other than a subscriber's email address confidential, unless the subscriber permits disclosure (opt-in). If a subscriber wants to keep his email address confidential, he must make the affirmative request, and the provider is required to give subscribers "conspicuous" notice of this right

⁹⁶ We also note that, while it is not a significant law applying generally to websites, Maine statutes (Section 1. 20-A MRSA §6001) prohibit public schools from publishing personal information about their students online prior to obtaining written parental consent.

⁹⁷ S.B. 485, 70th Leg., Chapt. 530 § 21 (Nev. 1999).

(opt-out). Providers face \$50 to \$500 fines for each misdemeanor. Any victim can bring a civil action to recover actual and punitive damages.

Earlier this year, **Virginia** passed the Internet Privacy Policy law,⁹⁸ which applies only to the websites of the state's agencies and public bodies. The statute mandated notice, but did not address consent. The law will require every public body that has an Internet website, including any organization in the state principally supported by public funds, to post a "conspicuous" privacy policy by January 1, 2001. The policy must describe at a minimum:

- (1) what information including personally identifiable information will be collected, if any;
- (2) whether any information will be automatically collected simply by accessing the website and, if so, what information;
- (3) whether the website automatically places a computer file, commonly referred to as a "cookie," on the Internet user's computer and, if so, for what purpose; and
- (4) how the collected information is being used or will be used.⁹⁹

Similarly, **Maryland** recently amended its laws (Section 10-624 and 10-633 Annotated Code of Maryland, effective October 1, 2000) to require government entities collecting information over the Internet to post their privacy policies and to ensure the security of the information that they have gathered. This law protects "personal information" such as; addresses, descriptions, finger or voice prints, numbers or pictures of an individual. The law also places a burden of proof on the state governmental entity collecting it to show a clear need for the information and that the information will only be used in a manner that is appropriate and relevant to the purpose for which it was collected.

State Bills Targeted at ISPs

Most state bills targeting Internet service providers require opt-in consent, which implicitly requires a form of notice. Contrary to five other states, **Michigan** adopts an opt-out approach to achieve consumer consent. Michigan's Internet Privacy Act¹⁰⁰ stalled in a House committee when introduced in February 1999 for the second time, following its inception in 1998. The bill requires Internet service providers to "notif[y] the customer in advance of its intention" to use customers' information and that the customer has the option to prohibit the use. However, it does not require a customer to consent in advance, thereby permitting providers to use information so long as they have notified customers (i.e., opt-out). Under the legislation, a violation is a misdemeanor offense with a fine of not more than \$100 and/or imprisonment for not more than 90 days. Those who put an individual's nonpublic information on the Internet with the intent to cause physical or financial

⁹⁸ H.B. 513, 2000 Sess. (Va. 2000).

⁹⁹ VA Code, Chapter 405, § 2.1-341.

¹⁰⁰ H.B. 4171, 90th Leg. (Mich. 1999).

harm, or distribute such information, are guilty of a felony punishable with a fine not greater than \$5000 and/or imprisoned for not more than two years. This legislation is not expected to move at all this session, which ends December 2000.¹⁰¹

The **Alaska** state legislature has proposed two bills aimed at Internet service providers; one endorses the opt-out approach and the other, the opt-in approach. House bill 410¹⁰² would require Internet service providers to notify subscribers of their policies regarding information access, and permitting subscribers to request their information remain confidential (opt-out). Violators are liable to the subscriber for damages or \$250. House bill 273¹⁰³ applies the more restrictive “opt-in” approach prohibiting those providers in the business of providing direct Internet access services from disclosing subscriber information to a third party without affirmative subscriber consent. Upon activation of a new account, providers must notify subscribers of these privacy restrictions, as well as whether the subscriber has provided its affirmative consent to disclose personal information. Subscribers can recover a \$500 damage award for each illegal disclosure.

Most state legislation targeting providers embrace the opt-in approach. **Five such state bills** (in California, Oklahoma, Kansas, Tennessee, Minnesota) effectively died at adjournment ending the last legislative session for each state. California, Oklahoma, and Kansas are examples of state bills that detail choice requirements, but lack an explicit notice element. The most recent attempt in **California** to implement an Internet privacy law¹⁰⁴ strictly prohibits Internet service providers from disclosing personally identifying information¹⁰⁵ about the subscribers (opt-in). The latest version of the bill, however, survived a red line edit with only its name and purpose. **Oklahoma's** Consumer Internet Privacy Protection Act¹⁰⁶ also conditionally permits those Internet computer services that provide computer access via modem to use personal information only if they achieve “prior informed written consent” from the subscriber (opt-in). Disclosure without consent is permissible when necessary to protect network security. The bill provides for

¹⁰¹ The bill was introduced by a Democratic Representative to a Republican-majority state legislature.

¹⁰² H.B. 410, 21st Leg. (Alaska 2000).

¹⁰³ H.B. 273, 21st Leg. (Alaska 2000).

¹⁰⁴ A.B. 1793, 1999-2000 Sess. (Ca. 2000).

¹⁰⁵ “‘Personally identifying information’ includes a subscriber’s electronic mail address, social security card number, date of birth, income, occupation, credit card or debit card information, current and prior addresses, telephone number, or mother’s maiden name. [It] also includes any information gathered by means of tracking an individual subscriber’s Internet usage, IP connection history, preferences, equipment, software, or user profile. [It] does not include aggregate data that cannot be used to identify an individual subscriber, or information disclosed by the Internet service provider to any of its affiliates or to a third party in connection with the processing, billing, collection, or maintenance of an individual subscriber’s account.” See A.B. 1793, 1999-2000 Sess. (Ca. 2000).

¹⁰⁶ H.B. 1651, 47th Leg., Reg. Sess. (Okla. 1999).

the state Attorney General to bring an action under the state Consumer Protection Act and permits subscribers to bring actions under the proposed bill. **Kansas's Internet Privacy Protection Act**¹⁰⁷ prohibits Internet access services from disclosing "personally identifying information"¹⁰⁸ about a Kansas subscriber to a third party" without affirmative consent (opt-in).

Tennessee and Minnesota are examples of state bills with both notice and consent elements. The **Tennessee Internet Personal Information Privacy Act**¹⁰⁹ requires online computer services¹¹⁰ to provide clear and conspicuous notice and obtain opt-in consent prior to disclosure of personal information. The bill, however, permits disclosure without consent if "necessary to render or conduct business or provide service to the subscriber." Willful or knowing illegal disclosure can result in damages not greater than \$1000. The **Minnesota Internet Privacy Bill**¹¹¹ requires interactive service providers, including those whose primary business it is to offer Internet access to consumers via telecommunications, to notify the consumer with a request for their informed consent (opt-in). Under the legislation, an ISP's violation would carry a damage award to the customer of \$500 or actual damages.

State Bills Targeted at Websites

State bills targeting websites' compliance with privacy standards require some form of notice to educate the customer about the site's information collection policies, by way of either clear and conspicuous notice or a privacy policy. The bills vary, however, on their approach to addressing consumer choice with opt-in and opt-out clauses. The **New York State Internet Privacy Law**¹¹² and the **Internet Privacy Policy Act**¹¹³ both reached the Senate in June 2000. The former bill prohibits a website from disclosing personal information without user consent (opt-in). Along with consent, a website

¹⁰⁷ H.B. 2896, 2000 Sess. (Kan. 2000).

¹⁰⁸ "'Personally identifying information' includes a subscriber's electronic mail address, social security number, date of birth, income, occupation, credit card or debit card information, current and prior addresses, telephone number, or mother's maiden name. [It] also includes any information gathered by means of tracking an individual subscriber's Internet usage, IP connection history, preferences, equipment, software or user profile. [It] does not include aggregate data that cannot be used to identify an individual subscriber, or information disclosed by the internet service provider to the third party in collection with the processing, billing, collection or maintenance of an individual subscriber's account." See H.B. 2896, 2000 Sess. (Kan. 2000).

¹⁰⁹ S.B. 2836, 101st Leg. (Tenn. 2000).

¹¹⁰ "'Online computer service' means the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing or making available information using computer-based telecommunications. Online computer services shall also include a service that permits a subscriber to retrieve stored information from or file information for storage in information storage facilities, electronic publishing or an electronic messaging service." See S.B. 2836, 101st Leg. (Tenn. 2000).

¹¹¹ S.F. 1716, 81st Leg. (Minn. 2000).

¹¹² S. 7754, 2000 Leg. (N.Y. 2000).

¹¹³ S. 5590-B, 223d Leg. (N.Y. 2000).

must also provide clear and conspicuous notice of the user's rights. The bill permits class actions and sets the minimum award requirement at \$500. The latter, the Internet Privacy Policy Act, requires all state agencies and any company doing business with New York to adopt Internet privacy policies that address the principles of notice, choice, access, and security.

Arizona legislation, like that of New York, also took an opt-in approach. An Arizona Internet privacy bill,¹¹⁴ which never left the House after its introduction in 1999, would require a website operator based in Arizona to fully disclose its privacy policy and conditions and to obtain from a website visitor its affirmative acceptance of the policy before the visitor can access a website's other pages (opt-in). The state attorney general could fine a violator up to \$5000 and any person can recover actual damages.

Other states are less clear on their intent to apply an opt-in or opt-out standard on websites. The **New Jersey Online Privacy Protection Act**,¹¹⁵ for example, would require websites to post clear and conspicuous notice of the website's personal information practices, but it does not embrace an **opt-in or opt-out** consent approach. The penalties for violations would include \$7500 in damages for the first abuse, and \$15,000 thereafter. In **Wisconsin**, an Internet privacy bill¹¹⁶ would require that a person maintaining a commercial website in the state to display on the homepage a privacy notice describing its information collection and use practices. The bill then applies an **opt-out** standard for all visitors, except for state residents who must **opt-in**. In both cases, damage awards can reach \$10,000 for each violation.

State Bills Targeted at Entities Holding Personal Information

Some state bills target neither websites nor Internet service providers directly, but rather organizations, any person, or information custodians. The **Hawaii Information Privacy Act**¹¹⁷ was created with an eye to the Internet, but applies generally to nongovernmental organizations' use of individual's information. The bill would require "appropriate" consent or approval under other specified conditions listed in the bill. Amendments to the original bill modified the opt-in consumer provision to an **opt-out** approach, which is more appealing to e-business. For violations, the bill would provide fines of not more than \$1000 for each offense or a maximum of \$50,000 for a business practice. No private right of actions are permitted. Similar to the Hawaii bill, **Vermont** generally targets "any person" who publishes personal identifying information, but unlike Hawaii, the Vermont bill adopts an **opt-in** approach. The Privacy of Person Identifying Information on the Internet bill¹¹⁸ succinctly prohibits a person from publishing personal identifying

¹¹⁴ H.B. 2690, 44th Leg. (Ariz. 1999).

¹¹⁵ A. 591, 209th Leg. (N.J. 2000).

¹¹⁶ S. 375, 1999 Leg. (Wis. 2000).

¹¹⁷ S.B. 2440, 2000 Leg. (Haw. 2000); H.B. 1877, 2000 Leg. (Haw. 2000).

information without consent. The bill does not define "person" or "publishing."¹¹⁹ **Washington** generally tailors its Privacy of Personal Information in Commercial Transactions bill¹²⁰ to address "information custodians,"¹²¹ including nonpublic commercial entities. The bill would permit transfer of personal information only if the website clearly and conspicuously posts a privacy policy where the consumer is informed that he may **opt-out**.

State Bills That Allude to Internet Privacy in General Privacy Bills

Other state bills focus on limiting the use of personal information, not particularly targeting Internet-related businesses, but alluding to technology concerns. For instance, **South Carolina's** Personal Information Privacy Act¹²² requires a person who discloses personal information whether online or offline, to obtain prior authorization from an individual who opts into permitting such disclosure. Penalties can include fines up to \$25,000 or up to 10 years imprisonment. A separate section in the bill establishes a joint legislative committee to study technology-related personal information privacy issues. **Delaware's** Senate bill¹²³ addresses financial institutions' responsibility to provide consumers with a clear, concise, and conspicuous disclosure statement, whether physical or electronic, regarding dissemination of their personal or financial information online or offline. The bill recognizes that information is provided to Internet marketing firms and explicitly requires a consumer to "first enter into" an "opt-in agreement" before their information is disseminated. Other states that have introduced legislation to create a body to study Internet privacy issues include Utah, Florida, Massachusetts, Nevada, New Mexico, Oregon, and Rhode Island.¹²⁴

¹¹⁸ H. 220, 65th Leg. (Vt. 1999).

¹¹⁹ *Id.* Bills in Colorado and Kansas, which have failed in the legislatures, would likewise prohibit the collection of personal information from Internet users without the user's consent. Colorado House Bill 00-1459; Kansas House Bill 2896.

¹²⁰ S.B. 6513, 56th Leg. (Wash. 2000).

¹²¹ An "information custodian" includes "all nonpublic commercial entities that maintain data containing personal information or sensitive information about consumers they know reside in Washington and that sell, share, or otherwise transfer the information to others, including affiliates or nonaffiliates, for purposes other than consumer-requested purposes or functional business purposes." *See id.* at § 2(7).

¹²² H. 4469, 113th Leg. (S.C. 2000).

¹²³ S.B. 252, 140th Leg. (Del. 1999).

¹²⁴ S.B. 1334, 32d Leg. (Fla. 2000); S. 1396, 181st Leg. (Mass. 1999); A.B. 364, 70th Leg. (Nev. 1999); S.B. 171, 44th Leg. (N.M. 1999); H. 2804, 70th Leg. (Or. 1999); R. 346, 2000 Leg. (R.I. 2000); H.B. 70, 53d Leg. (Utah 2000).

State Commissions Studying Privacy Issues

In addition to state legislation to regulate privacy, some states have established commissions to examine the issues of privacy on the Internet and report back to the state legislatures with recommendations.

In **Maine**, for example, the **Department of Administrative and Financial Services' Information Services Board (ISB)** is currently drafting an Internet privacy policy for state-owned websites. The ISB report will be presented to the incoming 120th Legislative Assembly, which commences on December 6, 2000. In addition to the ISB, the 1999 Maine legislature created a **Blue Ribbon Commission** to establish a comprehensive state “business and regulatory” Internet policy. The commission is recommending an addition to the ISB's policy that would require state agency websites, legislative websites, judicial websites, and municipal government websites to post a privacy policy on their sites. The commission has not yet made any recommendations regarding privacy protections for users of commercial websites, but this issue has been the topic of several recent commission meetings.

Similarly, **Maryland** created the **Maryland State Information Technology Board (ITB)** in 1999, which is empowered to develop standards and make recommendations concerning Internet user privacy including the availability of personal information on the Internet. The ITB presented a report to the legislature on January 6, 2000 recommending that Maryland adopt a host of core privacy principles. The ITB report also recommended that business and industry groups form an organization to certify sites as in compliance and to educate consumers about their privacy rights.

The **Oregon** legislature also created the **Oregon Internet Commission** in 1999, which will present final recommendations and a report to the 71st Legislative Assembly, which commences on January 8, 2001. While the commission's sunset date is December 31, 2000, the commission recommends the creation of a Legal Infrastructure Advisory Committee to further study Internet and technology issues. The commission report will recommend a “wait and see” approach to state privacy legislation, to avoid duplicative laws that will most likely be preempted by federal legislation currently pending before Congress.

Federal Legislation: Upcoming Nationwide Privacy Laws

The tensions between competing state and federal jurisdiction on information privacy and the Internet are certain to raise more congressional action in the next 107th session. At the federal level, the FTC is engaged in addressing the same conduct—Internet profiling—through industry consensus. The “profiling” issue exemplifies that some states are eager to apply particularized



legislation targeting Internet privacy to address constituent complaints, at the same time as federal efforts toward industry consensus proceed. The acknowledged problem with multiple state laws is the compliance issues for commercial businesses and the confusion and frustration for consumers, suggesting that a federal law may be the most appropriate solution. At the same time, while there are hundreds of **federal privacy bills** pending, a single preemptive federal law may also rob states of their consumer protection role.

Consumer Internet Privacy Enhancement Act

One recent bipartisan federal bill that attempts to resolve these many competing interests is the **Consumer Internet Privacy Enhancement Act**,¹²⁵ sponsored in the Senate by John McCain (R-AZ), John Kerry (D-MA), Barbara Boxer (D-CA), and Spencer Abraham (R-MI). This bill would require commercial website operators, online services who collect visitor information, or any other person selling online to post a clear, conspicuous, and easily understood notice describing their use of personally identifiable information.¹²⁶ The bill would also permit users to limit the use and disclosure of their information by **opting-out**. While states would be preempted from legislating more restrictive provisions, such as an opt-in clause, the bill would permit states to bring a civil action in federal district court on behalf of residents to enjoin a website's practices or obtain damages. The Federal Trade Commission could also bring an action as an unfair or deceptive trade practice to prevent a violation. In addition to other fines, a website faces a civil penalty of \$22,000 for each violation or each day of violation. However, the maximum penalty for a "related series" of violations is \$500,000. The bill also provides websites with a "safe harbor" provision, whereby the website is deemed to comply with the law if it complies with a self-regulatory seal program approved by the FTC. Finally, the act would direct further studies on the protection of information privacy.

Online Privacy Protection Act of 1999

Similarly, the **Online Privacy Protection Act of 1999**¹²⁷ sponsored by Senators Burns (R-MT) and Wyden (D-OR) would require website owners and online service providers (operators) to post a clear and conspicuous statement on the website concerning the personal information that is collected, how

¹²⁵ S. 2928, 106th Cong. (2000).

¹²⁶ "The term 'personally identifiable information' means individually identifiable information about an individual collected online, including—(A) a first and last name, whether given at birth or adoption, assumed, or legally changed; (B) a home or other physical address including street name and name of a city or town; (C) an e-mail address; (D) a telephone number; (E) a Social Security number; or (F) unique identifying information that an Internet service provider or operator of a commercial website collects and combines with any information described in the preceding subparagraphs of this paragraph." S. 2928, 106th Cong. at § 5(5).

¹²⁷ S. 809, 106th Cong.

the information is used, and what information may be shared with other companies. If the information is to be used in a manner inconsistent with the statement, then the operator must provide the user with the ability to object or **opt-out** to such use. This act would also require the operator to disclose the personal information collected or released to third parties, on request of the user. The act would also require the operator to have reasonable procedures for the security and confidentiality of the personal information. Under this act, the FTC would implement the law within one year of its enactment, and violations of the FTC rules would be subject to the FTC's authority as an unfair or deceptive act. The act would also preempt inconsistent state law directed at online privacy, but it would not preempt state law prosecutions for fraud.

Consumer Privacy Protection Act

By contrast, the **Consumer Privacy Protection Act** introduced by Senator Hollings (D-SC) would take a more comprehensive and pro-regulatory position toward consumer privacy protection.¹²⁸ The act would initiate a number of privacy studies and actions, and noted here are some of the more significant aspects of the act for commercial website privacy. This act would generally preempt inconsistent state laws. It also contains certain exceptions from state law preemption and would permit state law actions based on fraud, common law rights, tort law, and private rights of action under state consumer protection law, even when that law is otherwise preempted. The act applies broadly to commercial website owners, ISPs, online service providers, and third parties such as advertisers who collect information via a website (collectively "covered entities"). All covered entities must post on their websites a privacy policy. The covered entities would be prohibited from collection, use, or disclosure of personally identifiable information unless they obtain the consumer's prior affirmative consent. Thus, this act, in contrast to the other two bills summarized above, would impose an opt-in requirement on the collection, use, and disclosure of personal information. The covered entities must have measures in place to protect data security and must allow consumers with access to personal data in order to review and revise such data. The act provides for the FTC to establish rules implementing these privacy protections, and a violation of the act would be deemed an "unfair or deceptive act or practice" in violation of federal law. Further, the act would provide a number of other enforcement actions, such as: a private right of action in state court with statutory and punitive damages and attorneys fees; a state attorney general action in federal district court; "whistle-blower protection" for employees of covered entities that report on violations by their employer.

¹²⁸ S. 2606. 106th Cong.

The resolution of the competing privacy bills in Congress promises to be a contentious issue in the 107th Congress.

Conclusion

Keeping up with the panoply of state and federal privacy statutes, as well as privacy regulation or enforcement at the FTC and FCC, is a daunting task for any responsible company involved in commerce on the Internet. The laws are likely to be complex and to evolve over time. One fundamental first step that any company with a website can do, however, and a core theme in the law and the proposed law, is provide notice to users of the companies' practices regarding personal information. This can be accomplished through a privacy statement that explains the company privacy policy, such as how the user's personal information is used, collected, stored, and disclosed to third parties. With good legal counsel, the privacy statement should conform to industry fair information practices and anticipate trends in the law. The policy should be posted to the website for users to review, and the company should keep to the spirit and the letter of their stated privacy practices. Finally, it is important to be aware that the objective is *fair* use of your customer's information to promote reasonable and long-lasting relationships with your customer. The best way to assure a customer that its privacy will be respected is to define and post the company's privacy statement. Moreover, as the law changes, it is essential for companies to keep abreast, both to inform the debate on proposed laws and to avoid the risks of privacy litigation. As every parent learns, allowing the toddler to dip into the cookie jar in a controlled manner can be the best solution after all.