INTRODUCTION

The Internet economy is no longer a novelty. As of September 2012, approximately 81 percent of American adults use the Internet, and adults spend more time on the Internet than ever before. Nearly 90 percent of American households with computers have broadband connections at home. A recent poll revealed that most Internet users are concerned with the security of their personal information online, and 88 percent of the poll respondents believe legal protection of their privacy should be as strong online as it is offline. More than half of mobile application users polled have uninstalled or avoided certain apps due to privacy concerns.

Privacy and personal-data issues remain hot topics in the popular press, particularly as they relate to security breaches of financial or health information, unsolicited commercial e-mail (“spam”), and high-profile scandals involving issues such as “pretexting”—the practice of using deceptive means to obtain people’s telephone and other personal records without their knowledge or consent. Online businesses also pay attention as regulatory fines and consumer compensation costs mount for data breaches.

For example, ChoicePoint settled with the Federal Trade Commission (“FTC”) in 2006, paying $10 million in civil penalties and $5 million in consumer redress. Following large security breaches in 2003 and 2006, retailer TJX faced a regulatory complaint by the FTC, litigation brought by forty state attorneys general, and class action litigation. The company set aside a $107 million reserve to cover potential losses. It settled numerous class action lawsuits, providing some claimants with store vouchers and others with three years of credit monitoring services, credit insurance, and the cost of replacing driver’s licenses. In June 2009, the state attorneys general settled with

---

6 Press Release, TJX Companies, Inc., The TJX Companies, Inc. Reports Strong Second Quarter FY08 Operating Results; Estimates Liability from Computer Systems Intrusion(s) (Aug. 14, 2007), available at
TJX, resolving allegations that TJX’s data practices were faulty and did not adequately protect consumer information. As part of the settlement, TJX paid $9.75 million to the states and implemented a comprehensive information security program to address weaknesses in its computer security systems. Adverse publicity coupled with significant financial risks creates a perfect storm for regulatory activity.

Laws governing online privacy remain numerous and confusing as legislators, regulators, and law enforcement officials race to protect “privacy.” Congress continues to grapple with privacy-related legislation. Congress has already enacted legislation to protect financial and health information, as well as information about children under thirteen years old. As of December 2012, it is considering three bills proposing comprehensive federal privacy legislation, in addition to data breach, location privacy, and Do-Not-Track legislation.

Furthermore, the state attorneys general, the FTC, and plaintiffs’ class action lawyers have increased their activity in the privacy area. Nearly every state has adopted legislation requiring notice of security breaches, usually modeled after California’s breach notification statute. In response to concerns about privacy and identity theft, the FTC reorganized and created a new division called the “Privacy and Identity Protection Division.” The FTC released its Privacy Report and announces new initiatives and settlements almost monthly, as it cracks down on security lapses and uses its authority under Section 5 of the FTC Act to investigate companies that have not followed their privacy policies or have not made any express privacy or security promises. At the end of 2012, the FTC issued a report calling for simplified data collection and usage choices for consumers, greater transparency of privacy policies, and the implementation of privacy by design in business processes and IT systems.

To help understand the practical realities of this evolving environment, this article reviews and describes many of the key privacy-related statutes and regulatory regimes in the United States; notes some of the more significant lawsuits and private sector or government initiatives; analyzes the EU Data Protection Directive and the “Safe Harbor” framework instituted by the United States to address data transfers from Europe to the United States; and then submits some observations of this legal environment that should be of interest to businesses and their advisors.

This article provides a general survey of privacy law’s impacts on online commerce and discusses in greater detail many significant recent legal developments in the field. However, devoting significant attention to each development in this format simply is not possible. Please contact the authors with further questions and comments via e-mail.
# TABLE OF CONTENTS

INTRODUCTION.................................................................................................................................................1

TABLE OF CONTENTS ..............................................................................................................................................3

KEY FEDERAL PRIVACY LAWS .............................................................................................................................3

Constitutional Considerations ...............................................................................................................................5
  A. The Fourth Amendment and the Right to Privacy ......................................................................................5
  B. The First Amendment and Data-Related Privacy Developments ............................................................5
  C. Electronic Communications Privacy Act .....................................................................................................8
    A. Title I of the ECPA – the Wiretap Act ........................................................................................................9
    B. Title II of the ECPA – The Stored Communications Act ....................................................................9
Workplace Privacy ................................................................................................................................................10
  A. The Computer Fraud and Abuse Act ........................................................................................................10
  B. Title II of the ECPA ....................................................................................................................................13
Spam: Controlling the Assault of Non-Solicited Pornography and Marketing Act (“CAN-SPAM Act”) ..............14
Privacy of Financial Information ..........................................................................................................................15
  A. Gramm-Leach-Bliley Act ............................................................................................................................15
  B. Fair Credit Reporting Act ...........................................................................................................................19
Identity Theft .......................................................................................................................................................20
  A. Red Flags Rule .........................................................................................................................................21
  B. Pretexting ...............................................................................................................................................22
Children’s Privacy: COPPA, COPA, and the PROTECT Our Children Act ....................................................23
  A. Children’s Online Privacy Protection Act ..................................................................................................23
  B. Child Online Protection Act .......................................................................................................................26
  C. PROTECT Our Children Act ......................................................................................................................26
Personal Health Information: Health Insurance Portability and Accountability Act ...........................................27
Telephone Consumer Protection Act ..................................................................................................................31
Cable Communications Act .................................................................................................................................31
White House’s Privacy Framework .....................................................................................................................32
Other Federal Statutes .......................................................................................................................................33

KEY STATE PRIVACY LAWS ...........................................................................................................................33
State Constitutions ..............................................................................................................................................34
“Spam” .............................................................................................................................................................34
Identity Theft .......................................................................................................................................................35
Privacy Policies ....................................................................................................................................................35
Data Breach Notification ...................................................................................................................................35
State Common Law ..........................................................................................................................................37

FTC ENFORCEMENT AND INITIATIVES ...........................................................................................................37
Organization and Authority................................................................................................................................37
KEY FEDERAL PRIVACY LAWS

Constitutional Considerations

In the United States, the Constitution and Bill of Rights provide U.S. citizens with rights against the government. Some of these rights fall within the umbrella right to privacy. The Constitution also sets the minimum requirements a plaintiff must meet to enforce these rights in federal court.

A. The Fourth Amendment and the Right to Privacy

Generally, the Fourth Amendment to the Constitution protects individuals from unreasonable searches and seizures by the government. To invoke the protections of the Fourth Amendment for the content of communications, a person must have a “reasonable expectation of privacy” in the communications at issue. Under the *Katz* test, a reasonable expectation of privacy exists where (1) a person has exhibited an actual (subjective) expectation of privacy; and (2) society recognizes the expectation as a reasonable one.

As it relates to the digital age, the Fourth Amendment prevents the government from searching the contents of email and other information stored on a person’s personal computer system without proper justification and procedures. Courts have concluded that email senders have a reasonable expectation of privacy in the contents of their messages in most circumstances, but they do not have a reasonable expectation of privacy in the emails’ addressing information of the emails, such as IP addresses or to/from addresses. However, even when a court determines that an individual has a reasonable expectation of privacy in his email communication or computer data, government authorities still may search and seize it when such actions are reasonable under the circumstances.

One common situation where email communications are monitored is in the workplace. Employers commonly monitor employees’ email and Internet use, which raises privacy concerns. Generally, Fourth Amendment protections directly apply only to government employees. However, the *Katz* test has heavily influenced how courts view privacy-related claims brought against private actors under federal and state law. Due to the limited constitutional privacy protections for electronic and other communications, Congress, federal regulators, and state legislators have pushed for more privacy protections. The bulk of this article discusses many of them.

B. The First Amendment and Data-Related Privacy Developments

In addition to Fourth Amendment considerations, free speech and related First Amendment considerations increasingly arise in connection with identification of users and data subjects. Many Internet users believe that an important feature of the Internet is a person’s ability to use it anonymously. ISPs market privacy-related features, and some promise, in their privacy policies, to conceal users’ identities to the fullest extent allowed by law. The Supreme Court has recognized the right to speak and act anonymously in the context of political speech, however, privacy rights can come into conflict with other rights.

---

17 *Id.*
18 *See* United States v. Charbonneau, 979 F. Supp. 1177 (S.D. Ohio 1997) (stating that individual may have reasonable expectation of privacy in content of e-mails, but no reasonable expectation of privacy in e-mail sent to participants in a chat-room); Stengart v. Loving Care Agency, Inc., 29 ILR (P&F) 399, 990 A.2d 650 (N.J. 2010) (holding that employee had reasonable expectation of privacy in e-mail communications with her lawyer through her personal account, even where that account was accessed using employer-owned computer equipment); United States v. Maxwell, 2 ILR (P&F) 258, 45 M.J. 406, 412-17 (C.A.A.F. 1996). *See also* Davis v. Gracey, 1 ILR (P&F) 190, 111 F.3d 1472 (10th Cir. 1997) (holding that police warrant authorizing seizure of computer is sufficiently broad to cover electronic communications stored in the computer); *but cf.* Guest v. Leis, 8 ILR (P&F) 375, 255 F.3d 325 (6th Cir. 2001) (holding there is no reasonable expectation of privacy in postings to bulletin board); State of New Jersey v. Evers, 13 ILR (P&F) 224, 815 A.2d 432 (N.J. Sup. Ct. 2003) (holding there is no reasonable expectation of privacy in e-mail sent to chat room participants).
19 *See* Forrester v. United States, 512 F.3d 500, 510-11 (9th Cir. 2008) (holding that Fourth Amendment did not prohibit government interception of IP addresses of websites visited and to/from addresses of e-mails); *but cf.* In re Application of the United States for an Order Authorizing the Release of Historical Cell-Site Information, No. 10-MC-897 (NCG), 2011 WL 3678934, at *3-13 (E.D.N.Y. Aug. 22, 2011) (holding that cell-phone users had reasonable expectation of privacy in location of cell towers from which calls were made, despite information being held by third-party service provider).
A leading example of the tension between protecting the privacy rights of Internet users and the intellectual property rights of copyright holders arose in connection with peer-to-peer music sharing. In *In re Verizon Internet Services,* 21 the Recording Industry Association of America (“RIAA”) served a subpoena issued pursuant to a Digital Millennium Copyright Act (“DMCA”) claim, demanding that the Internet Service Provider (“ISP”), Verizon, disclose the identities of two Verizon users suspected of offering pirated music downloads over Verizon’s network. 22 Verizon resisted the subpoena, but the trial court rejected Verizon’s privacy and constitutional arguments and ordered Verizon to divulge the names. 23 The trial court conceded, however, that “there is some level of First Amendment protection that should be afforded to anonymous expression on the Internet, even though the degree of the protection is minimal where alleged copyright infringement is the expression at issue.” 24 On appeal, rather than focusing upon the constitutional implications, the Court of Appeals for the D.C. Circuit reversed the trial court ruling that the DMCA does not authorize the issuance of a subpoena to an ISP [Verizon], when it acts only as a conduit for communications and does not store the material. 25

Beyond issues relating to user anonymity, commercial speech interests relating to the collection and use of data also increasingly arise. The Supreme Court recently relied upon the First Amendment to strike down legislation partially directed at privacy concerns. In *Sorrell v. IMS Health, Inc.,* the Supreme Court held that a Vermont statute prohibiting pharmacies from selling information about doctors’ prescribing practices for the purposes of marketing was an unconstitutional restraint on speech. 26 Notably, this statute did not focus on protecting the privacy of patients’ information, it was directed at doctors’ information. 27 One of the businesses it most affected was data aggregators who purchased the information from pharmacies, analyzed it, and sold aggregated numbers to pharmaceutical drug manufacturers. 28 The court found that the law was both a content and viewpoint based restriction on commercial speech, which resulted in heightened analysis. 29 The court rejected both of the state’s justifications for the law. It rejected the justification that it advanced the goal of lowering medical services costs and promoting public health. 30 It also rejected the state’s argument that the law protected doctors’ interests in “keeping their prescription decisions confidential,” because the statute allowed information to be sold for any other purpose, like medical research. 31 As the court said, “the State gives possessors of the information broad discretion and wide latitude in disclosing the information, while at the same time restricting the information’s use by some speakers and for some purposes . . .” 32 Under the guise of privacy protection, Vermont seemed to attempt to restrict a business model the state did not support. States may enact privacy regulation similarly in the future, which could lead to more uncertainty and complexity in the field, but in the wake of *Sorrell* it seems possible that additional constitutional challenges to such legislation may be likely.

C. Standing and Sufficiency of Complaint

Defendants have vigorously resisted the rising tide of privacy-related consumer class actions attempting to defeat them early and prior to accumulating massive discovery expenses. Constitutional challenges to plaintiffs’ standing have become common. A plaintiff must meet constitutional “standing” requirements for a federal court to have jurisdiction over a case. 33 Those requirements can be difficult to meet when asserting claims arising out of or

---

22 *In re Verizon Internet Services,* 257 F. Supp. 2d at 246.
23 *Id.* at 275.
24 *Id.* at 260.
25 *Recording Industries Association of America,* 351 F.3d at 1233. See also *In re Charter Communications,* Inc., *Subpoena Enforcement Matter,* 393 F.3d 771 (8th Cir. 2005) (holding the same).
27 *Id.* at 2668.
28 *Id.* at 2660.
29 *Id.* at 2663-64.
30 *Id.* at 2671.
31 *Id.* at 2668.
32 *Id.* at 2672.
relating to privacy.\textsuperscript{34} To have standing,\textsuperscript{35} a plaintiff must allege a sufficient injury by establishing that his injury is (1) an injury in fact that is (a) concrete and specific and (b) not hypothetical, but actual or imminent; (2) traceable to the defendant’s action; and (3) likely to be remedied by a favorable court ruling.\textsuperscript{36} Many of the class action lawsuits asserting technology-related privacy violations have failed to allege an injury sufficient to establish standing. Similarly, courts dismiss cases at the pleading stage due to plaintiffs’ failure to allege the minimum damages required by statute.\textsuperscript{37} Consequently, parties filing or replying to privacy actions should pay particular attention to the theory of damages laid out in the complaint.

The recent \textit{In re iPhone Application Litigation}\textsuperscript{38} decision illustrates the centrality of standing requirements for many of these cases. The trial court dismissed the case, because the plaintiffs failed to allege sufficient facts establishing standing.\textsuperscript{39} The plaintiffs alleged that Apple violated their privacy rights by allowing applications on the iPhone to access, use, and track their personal information.\textsuperscript{40} They alleged three types of injury: (1) misappropriation or misuse of their personal information; (2) diminution in value of their personal information, which they alleged was an “asset of economic value” due to its scarcity; and (3) “lost opportunity costs” in having installed the applications making their devices less secure and less valuable in light of the privacy concerns.\textsuperscript{41} The trial court found that the plaintiffs failed to allege an injury to themselves when they failed to identify the devices they used, which defendants accessed or tracked their personal information, and any harm that resulted from the alleged access or tracking of their personal information.\textsuperscript{42} The court also stated that the plaintiffs failed to show how

\begin{italicized}

\textsuperscript{34} \textit{See, e.g.}, Bell v. Axiom Corp., No. 06 Civ. 485, 2006 WL 2850042 (E.D.Ark. Oct. 3, 2006); Randolph v. ING Life Ins.

\textsuperscript{35} U.S. Const. art. III, § 2, cl. 1.


\textsuperscript{37} \textit{See, e.g.}, Birdsong v. Apple, Inc., 590 F.3d 955, 960-61 (9th Cir. 2009) (“The plaintiffs have not shown the requisite injury to themselves [that they had experience hearing loss as a result of the defendant’s product] and therefore lack standing [under Article III.]”); \textit{In re JetBlue Airways Corp., Privacy Litig.}, 379 F. Supp. 2d 299, 327 (E.D.N.Y. 2005) (holding that airline’s disclosure of passenger data to third party in violation of airline’s privacy policy had no compensable value); \textit{In re DoubleClick Inc. Privacy Litig.}, 154 F. Supp. 2d 497, 525 (S.D.N.Y. 2001) (holding that value of attention and demographic information was not an economic loss sufficient to count towards statutory damage requirement); La Court v. Specific Media, Inc., No. SACV 10-1256-GW(JC)X, 2011 WL 2473399, at *4-6 (C.D. Cal. Apr. 28, 2011) (holding that plaintiff failed to establish standing due to failure to allege economic harm from defendant’s cookie tracking to a specific plaintiff); Doe 1 v. AOL LLC, 719 F. Supp. 2d 1102, 1109 (N.D. Cal. 2010) (finding standing when plaintiffs’ alleged that AOL continued to publicly disclose plaintiffs’ highly sensitive personal information, including credit cards and social security numbers). Alleging damages is a common problem under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, and is addressed in more detail in that section.

\textsuperscript{38} \textit{In re iPhone Application Litig.}, No. 11-MD–02250–LHK, 2011 WL 4403963 (N.D. Cal. Sept. 20, 2011).

\textsuperscript{39} \textit{Id.} at *1-2.

\textsuperscript{40} \textit{Id.} at *3.

\textsuperscript{41} \textit{Id.} at *6.

\textsuperscript{42} \textit{Id.} at *6.

\end{italicized}
Apple caused the alleged harm when it simply provided a technology platform and did not itself allegedly misappropriate any data. 43

Plaintiffs must be able to identify specific personal harm from a privacy violation before a court will assert jurisdiction over their suit. Harm from privacy violations can be difficult to quantify, because much of the economic damage occurs indirectly or is the result of some further criminal act, such as identity theft, where determining causation can be difficult. Standing is just one of many obstacles plaintiffs must overcome to properly assert a privacy violation.

Consumer class actions relating to privacy continue to trend upwards,44 and constitutional challenges seem likely on all sides as the stakes increase.

Electronic Communications Privacy Act

In addition to constitutional considerations, numerous federal statutes also provide privacy protections online and elsewhere. Congress enacted the Electronic Communications Privacy Act of 1986 (“ECPA”)45 to extend protections of the federal wiretapping statute to electronic communications. In general, the ECPA prohibits the unauthorized access, disclosure, and use of electronic communications whether in transit or in storage. Title I of the ECPA (often referred to as the Wiretap Act)46 prohibits the interception of electronic communications as they are in transit. However, the ECPA exempts from liability service providers who intercept a “wire, oral, or electronic communication . . . where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.”47 Title II of the ECPA (also called the Stored Communications Act or “SCA”)48 prohibits unauthorized access to stored communications.49 Title II primarily applies to ISPs and other entities offering “remote computing” services “to the public.”50 Some court decisions suggest the ECPA may also limit an employer’s ability to intercept or access e-mail messages on its private network.51 However, some commentators argue that the ECPA was not intended to govern electronic communications on private networks,52 though the ECPA’s text contains no such blanket exception.53

43 Id. at *9.


47 § 2511(2)(d).

48 §§ 2701-2712.

49 With respect to public communications service providers, the ECPA restricts disclosure of the identity of a subscriber, as opposed to the contents of a communication, only when the recipient is a “governmental entity.” 18 U.S.C. § 2703(c); Jessup-Morgan v. America Online, Inc., 20 F. Supp. 2d 1105 (E.D. Mich. 1998).


51 See Bohach v. City of Reno, 932 F. Supp. 1232, 1236 (D. Nev. 1996) (discussing application of the ECPA Title I and Title II requirements to city government employee e-mails); Cornerstone Consultants, Inc. v. Production Input Solutions, L.L.C., No. C 10–3072–MW1, 2011 WL 1899372, at *19-23 (N.D. Iowa 2011) (holding that the question of whether a subcontractor e-mail services provider or employer was the administrator of communications services is a factual question under 18 U.S.C § 2701(c)); but see Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 115 (3rd Cir. 2003) (citing Bohach, 932 F. Supp. at 1236; 18 U.S.C. § 2701(c) (holding that an employer did not violate Title II because it was a communications service provider under the statute).


A. Title I of the ECPA – the Wiretap Act

Title I prohibits the interception of electronic communications while they are in transit. In In re Pharmatrak, Inc. Privacy Litigation, the First Circuit ruled that the ECPA prohibits third parties from collecting personal information of Internet users without their consent. Pharmatrak contracted with pharmaceutical companies to monitor the traffic on their websites. In addition to collecting anonymous usage data, Pharmatrak also collected personally identifying information without the knowledge or consent of users or the pharmaceutical companies. The users of the pharmaceutical company websites alleged that such collection violated the website privacy policies. Reasoning that its contracts with the pharmaceutical companies constituted de facto “consent” to the collection of personal information under the ECPA, the trial court granted summary judgment in favor of Pharmatrak. The First Circuit reversed, holding that Pharmatrak violated the ECPA where it intentionally “intercepted” users’ personal information without their consent. The First Circuit did not address whether web monitoring of personally identifying information necessarily violates the ECPA if it is prohibited by a website’s privacy policy.

Title I allows ISPs to intercept communications if a party consents, and the First Circuit confirmed that Internet users can consent to the monitoring of their activity. There are two consequences of these rules. First, website operators can obtain consent to monitor their users’ actions on their public websites. Second, even if the ECPA applies to private networks run by employers, employers can likely avoid liability under the ECPA by requiring that employees sign a consent form allowing the employer to monitor their online activity.

B. Title II of the ECPA – The Stored Communications Act

Title II prohibits the unauthorized access of stored communications. Title II has a notable exception; it does not prohibit the search of stored e-mail when it is “authorized by the person or entity providing a wire or electronic communications service.” In Fraser v. Nationwide Mutual Insurance Co., the Third Circuit concluded that a company administering its own file server constituted a “communications service provider” under the ECPA. A company, therefore, does not incur liability for searching its own server for e-mails. This holding is especially important for employers that administer their servers, because they can search the employee e-mail stored on them. Title II’s application to the workplace context is discussed in more detail in a later section of this article.

Classifying the status of an electronic communication as “in transit” or “in storage” has important consequences. As the foregoing showed, Title I requires a user’s consent before intercepting a communication in transit is allowed. Title II requires only the server administrator to consent to a search of stored information. Users would likely want to classify their communications as in transit, while businesses would likely want to classify communications as in storage.

---

54 In re Pharmatrak, Inc. Privacy Litigation, 329 F.3d 9 (1st Cir. 2003).
55 Id. at 20.
56 Id. at 12.
57 Id. at 15-16.
58 Id. at 12.
60 In re Pharmatrak, 329 F.3d at 22-23.
61 Twelve states have all party consent rules where all parties that are part of a communication must consent before it can be recorded. Citizen Media Law Project, Recording Phone Calls and Conversations, http://www.citmedialaw.org/legal-guide/recording-phone-calls-and-conversations (last visited Nov. 1, 2011). Some class action cases have been filed for an alleged failure to abide by these rules. See Marquis v. Google, Inc., No. 11-2808 (Mass. Sup. Ct. July 29, 2011) (suing Google pursuant to Massachusetts’s all party consent law, Mass. Gen. Laws Ann. Ch. 272, § 99, for scanning emails sent to Gmail email accounts from people who do not have Gmail email accounts and thus have not consented to Google’s scan).
62 See United States v. Simons, 29 F. Supp. 2d 324 (E.D. Va. 1998) (stating that government employee consented to e-mail policy expressly giving employer authority to monitor usage); Deal v. Spears, 980 F.2d 1153 (8th Cir. 1992) (stating that consent will not be implied under the ECPA); accord Watkins v. L.M. Berry & Co., 704 F.2d 577 (11th Cir. 1983).
64 Fraser, 352 F.3d at 115.
65 Id.
In 2005, the First Circuit wrestled with placing the line between transit and storage in *United States v. Councilman*. In *Councilman*, the court considered the specific question of whether it is possible to “intercept” an electronic communication while in transit, but temporarily in storage. The court held that “the term ‘electronic communication’ [as used in Title I] includes transient electronic storage that is intrinsic to the communications process.” Therefore, intercepting an e-mail in transient storage violates the Wiretap Act. The legal classification of an electronic communication’s status as “in transit” or “in storage” generates different treatment under the ECPA. The policy question regulators face is whether it should.

These policy questions become more important as technology advances and the line between transit and storage blurs. The growth of cloud computing is one such technology advance. As cloud computing becomes mainstream, privacy advocates and industry representatives have called for ECPA reform to protect Internet users’ privacy interests. The Center for Democracy & Technology (“CDT”) has organized an industry-backed coalition, the Digital Due Process Coalition, to encourage reform. Three key principles of the reform are (1) access to the content of electronic communications should require a court order based on probable cause; (2) the ECPA should similarly regulate communications in transit or storage, as well as communications using various technology and platforms; and (3) the reformed ECPA should be simple and clear. In 2011, Senator Patrick Leahy (D-CT) introduced a Senate bill to amend the ECPA, which is supported by the Digital Due Process Coalition. While technology has yet to push the ECPA to its breaking point, technological change likely will continue to drive legislative reform in this area.

**Workplace Privacy**

The pervasive use of computers in the workplace creates conflicts over restricted access to information and employee privacy. Federal courts try to strike a balance between the rights of employers and employees. Two federal statutes frequently affect employee computer usage and related disputes: the Computer Fraud and Abuse Act (“CFAA”) and Title II of the ECPA.

**A. The Computer Fraud and Abuse Act**

The CFAA prohibits unauthorized use of computer systems and websites. Congress originally intended to combat computer hacking with the CFAA, so the statute primarily imposes criminal penalties, but it also provides for civil remedies in some circumstances. To bring a civil action under the CFAA, the plaintiff must show the defendant intentionally used a protected computer without authority or in excess of authority causing at least $5,000 in damages within a one-year period. Two common types of cases arise under the CFAA: (1) access to computer systems by former employees, and (2) data scraping by competitors and aggregators of online information.

---

66 United States v. Councilman, 418 F.3d 67 (1st Cir. 2005).
67 Id. at 69.
68 Id. at 79.
69 Id.
74 Protected computers are those used in or which affect interstate or foreign commerce or communication. 18 U.S.C. § 1030(e)(2)(B). The CFAA also protects computers used by a financial institution or the federal government. § 1030(e)(2)(A). Connecting to the Internet is sufficient to establish that a computer can affect interstate commerce under the CFAA. U.S. v. Drew, 259 F.R.D. 449, 458 (C.D. Cal. 2009) (in a criminal context); Patrick Patterson Custom Homes, Inc. v. Bach, 586 F. Supp. 2d 1026, 1034 (N.D. Ill. 2008) (in a civil context).
75 § 1030(a). Of the most common subsections used in civil actions, subsections (a)(2)(C) and (a)(4) allow for a violation when the user exceeds his or her existing authority, whereas subsection (a)(5) requires access without authorization. A minority of courts have read the CFAA to restrict civil actions to violations of 18 U.S.C. § 1030(a)(5). See Hot Stuff Foods, LLC v. Dornbach, 726 F. Supp. 2d 1038, 1045 (D. Minn. 2010).
76 18 U.S.C. § 1030(g), (c)(4)(A)(i)(I). Plaintiffs may also bring civil suits if the damage resulted in
Employers frequently bring claims under the CFAA against former employees who use their employers’ computers to help start a competing business. Courts originally sided with employers and held that an employee acted “without authorization” or “in excess of authorization” when he used his employer’s computers to access data during the term of employment, and the employee used that data adverse to his employer’s interest. Few courts continue to follow this line of reasoning. For example, in International Airport Centers, L.L.C. v. Citrin, the Seventh Circuit held that the CFAA created a cause of action against a former employee who was hired to collect data, irretrievably deleted it from his work laptop before returning the laptop to his employer, and subsequently started a competing business. The Seventh Circuit applied the common law of agency and reasoned that a former employee’s authorization to use the laptop terminates when the employee violates his duty of loyalty.

Recently, however, courts usually dismiss these types of claims. In LVRC Holdings LLC v. Brekka, the Ninth Circuit declined to apply the Seventh Circuit’s deauthorization-by-disloyalty analysis. In Brekka, a company alleged that a consultant accessed the company’s website in excess of his authorization when he used the company’s website to perform research necessary to start a competing company. The Ninth Circuit recognized that an employee may “exceed authorized access” if he accesses data for which he is not explicitly authorized, but the court held that an employee does not act “without authorization” under the CFAA if the employee has authorization to use a computer, regardless of his intentions.

Screen scraping or data scraping is the use of an automated program to extract data from a website by copying the data that appears on its web pages. Under current case law, courts have found that the CFAA imposes liability for screen scraping when a program circumvents password authentication on a website, the program exceeds the authority granted by a password protected website’s terms of use, or the scraping violates some other legal restriction. A website requiring click-through acknowledgment of its terms of use may also be sufficient to create liability for screen scraping under the CFAA. In America Online, Inc. v. LCGM, Inc., the Eastern District of

(II) the modification or impairment, potential modification or impairment of the medical examination, diagnosis, treatment, or care of 1 or more individuals;
(III) physical injury to any person; a threat to public health or safety;
(IV) damage affecting a computer used by or for an entity of the United States Government or in furtherance of the administration of justice, national defense, or national security; or damage affecting 10 or more protected computers during any 1-year period.

§ 1030(c)(4)(A)(i)(II)-(V).
Virginia held that an e-mail spammer exceeded its authority when it violated America Online’s terms of service by scraping e-mail addresses of America Online’s users from its password protected website.91 In EF Cultural Travel BV v. Explorica, Inc.,92 the First Circuit concluded that a former employee exceeded his authority under the CFAA to access his employer’s travel agency website, because he violated a confidentiality agreement with the travel agency by using the scraped pricing data to compete with it.93

Many courts have not extended liability under the CFAA to users who have authority to access the data, but allegedly scrape and misuse it in a manner objectionable to the website.94 For example, in Cvent, Inc. v. Eventbrite, Inc., the Eastern District of Virginia allowed an event planning website to scrape meeting venue data from a competitor.95 The court distinguished America Online, because in Cvent, the meeting venue data was publically available, unprotected by a password or click-through requirement to consent to the website’s terms of use prohibiting screen scraping.96 The court held that the screen scraping competitor did not violate the CFAA, because it did not obtain unauthorized access to the data, it only may have made unauthorized use of it.97

Under the CFAA’s most commonly used theory of recovery, the plaintiff must allege “economic damages” totaling at least $5,000.98 Courts have struggled to define the costs that may be considered to calculate the economic damages.99 The Ninth Circuit laid out an increasingly popular definition in Creative Computing v. Getloaded.com LLC.100 In that case, the court broadly defined “economic damage” as the value of property lost or money spent to recover that property.101 Under this broad definition, for example, courts have allowed plaintiffs to include the cost of hiring computer consultants to recover lost data and perform forensic tests to determine the extent of the harm to a computer system.102

Other courts use a much more limited definition of “economic damages.” Those courts only allow costs with a close nexus to an interruption in computer service caused by the CFAA violation.103 For example, in Nexans Wires S.A. v. Sark-USA, Inc.,104 the Second Circuit affirmed the trial court’s dismissal of a CFAA claim for failure to allege economic damages. In that case, former employees accessed their employer’s computer without authorization

90 America Online, 46 F. Supp. 2d 444.
91 Id. at 450-51.
92 EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577 (1st Cir. 2001).
93 Id. at 582-83.
94 Id. at 932-33.
95 Cvent, 739 F. Supp. 2d at 930.
96 Id. at 932.
97 Id. at 933 (citing State Analysis, 621 F. Supp. 2d at 317).
98 18 U.S.C. § 1030(g).
99 See, e.g., America Online, Inc v. National Health Care Discount, Inc., 121 F. Supp. 2d 1255, 1273-74 (N.D. Iowa 2000) (finding a triable issue in whether cost to America Online for loss of storage space due to defendant’s spam e-mail contributed to damage requirement); Lasco Foods, Inc. v. Hall and Shaw Sales, Mktg., & Consulting, 600 F. Supp. 2d 1045, 1051-52 (E.D. Mo. 2009) (holding that deletion of information from computer and cost of remedial measures required to retrieve and analyze defendant’s computer constitute loss under CFAA).
100 Creative Computing v. Getloaded.com LLC, 386 F.3d 930 (9th Cir. 2004).
101 Id. at 935.
102 See A.V. ex rel. Vanderhye v. iParadigms, LLC, 562 F.3d 630, 646 (4th Cir. 2009) (citing Creative Computing, 386 F.3d at 935) (holding that costs of security investigation and security changes in reaction to unauthorized computer access were not actionable under CFAA); Contract Assocs. Office Interiors, Inc. v. Ruiter, No. CIV. S-07-0334 WBS EFB, 2008 WL 3286798, at *3 (E.D. Cal. Aug. 6, 2008) (citing Creative Computing, 386 F.3d at 935) (holding that deletion of information from computer and cost of remedial measures required to retrieve and analyze defendant’s computer constitute loss under CFAA).
103 See Nexans Wires S.A. v. Sark-USA, Inc., 166 Fed. Appx. 559, 562-563, (2nd Cir. 2006) (affirming summary judgment for defendant because plaintiff did not claim loss of computer system service); Resdev, LLC v. Lot Builders Ass’n, No. 6:04-CV-1374ORL31DAB, 2005 WL 1924743 (M.D. Fla. Aug. 10, 2005) (holding that lost revenues from a stolen trade secret are not a “loss” under the CFAA, because the lost revenues are not a proximate consequence of unauthorized computer access); Costar Realty Information, Inc. v. Field, 737 F. Supp. 2d 496 (D. Md. 2010) (holding that lost revenue resulting from interruption in real estate company’s website was a “loss.”) Global Policy Partners, LLC v. Yessin, 868 F. Supp. 2d 642, 653 (E.D. Va. 2010) (holding that a real estate company’s claim of lost revenue is not “loss” under CFAA, because lost revenue resulted from the misappropriation of information and not the interruption in real estate company’s website).
to obtain trade secrets. The employer alleged that the economic gains to the former employees through unfair competition were economic damages under the CFAA. The trial court disagreed and dismissed the claim, citing the CFAA's statutory requirement that economic damage result from an “interruption of service.” Website operators should choose their jurisdiction carefully when making a CFAA claim.

B. Title II of the ECPA

As discussed above, private employers may legally review employee communications stored on company managed servers when the employer has provided notice of such monitoring, typically through an electronic resources policy. In essence, employees give up their expectation of privacy in the communications made with employer-provided equipment. In City of Ontario, California v. Quon, the Supreme Court addressed for the first time whether employers may review communications transmitted by and stored on the servers of a third party provider. In its Computer Usage, Internet, and E-Mail Policy (“the Policy”), the Ontario Police Department reserved the right to monitor and log network activity. The Policy stated that employees had no expectation of privacy when using the police department’s electronic resources, and the police department reserved the right to audit employee usage. The police department implemented the Policy before it purchased pagers for its employees, and consequently the Policy did not explicitly address text messages or pagers. However, at a staff meeting followed by a written memorandum, a managing officer clearly communicated to the employees that the Policy applied to the pagers. While it did not make a definitive finding, the Supreme Court suggested that the Policy extended to the text messages transmitted on the pagers, because the police department clearly extended the policy to the pagers. Consequently, the police department could monitor its employees’ communications over the pagers. As a result of this case, employers may be able to extend their electronic resources policies to include employee communications transmitted through a third-party service provider, such as a wireless phone provider or a third-party e-mail provider.

Because Quon dealt with a government employer, the case also had Fourth Amendment considerations. In Quon, following the police department’s written extension of the Policy to the use of employer-issued pagers, the same managing officer who wrote the Policy extension memorandum told employees that he did not intend to monitor the text messages transmitted with the pagers. The Ninth Circuit concluded that the manager’s statements created an expectation of privacy on the part of employees and eroded the city’s position despite its written policy. The Supreme Court declined to address this issue, noting that “[a] broad holding concerning employees’ privacy expectations vis-à-vis employer-provided technological equipment might have implications for future cases that cannot be predicted.” Accordingly, the Supreme Court assumed for the purposes of its analysis that the employee had a reasonable expectation of privacy under the Fourth Amendment in the messages transmitted on his government employer-provided pager. Nevertheless, the Court concluded that the search was reasonable for business reasons and committed no invasion of privacy. While the particular issue of whether a government employee has a constitutionally protected expectation of privacy under the Fourth Amendment in communications transmitted using an employer-issued device remains open, the Supreme Court has stated that government employees have an expectation of privacy in the contents of their desk and file cabinets. Therefore, to avoid

---

105 Id. at 472.
106 Id. at 477.
107 Id. (citing 18 U.S.C. § 1030(e)(11)).
109 Id. at 2625.
110 Id.
111 Id.
112 Id.
113 See id. at 2629.
114 See id. at 2625.
115 Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892, 908 (9th Cir. 2008).
116 Quon, 130 S. Ct. at 2630.
117 Id.
118 Id. at 2632-33.
possible Fourth Amendment violations, government employers should assume they need an employee’s consent before they monitor employees’ communications.

**Spam: Controlling the Assault of Non-Solicited Pornography and Marketing Act (“CAN-SPAM Act”)**

Congress created one national standard for the regulation of spam when it enacted the CAN-SPAM Act of 2003. The CAN-SPAM Act applies to all “commercial electronic mail messages,” which the statute defines as “any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service.” It exempts “transactional or [customer] relationship messages.” The CAN-SPAM Act imposes civil and criminal penalties on violators who send the commercial e-mail or advertise within the e-mail. Finally, it preempts state laws that expressly regulate the transmission of commercial e-mail, except where such laws target false or deceptive e-mail content.

To avoid civil liability under the CAN-SPAM Act, senders of commercial e-mail messages must meet the following requirements:

- **Do not have false or misleading e-mail header information or deceptive message subject lines.** Each e-mail message’s “to,” “from,” and routing information—including the originating domain name and e-mail address—must be accurate and identify the entity that initiated the e-mail. Further, the subject line of a commercial message cannot mislead the recipient about the contents or subject matter of the message.

- **Include a return address or other Internet-based opt-out method in all messages.** The commercial email sender must provide a return e-mail address or other Internet-based response mechanism that allows the e-mail recipients to ask the sender not to send future e-mail messages to their e-mail address, and the sender must honor all requests. The opt-out mechanism must be able to process opt-out requests for at least thirty days after the e-mail message is sent. The sender must process opt-out requests within ten business days. An opt-out request must be as simple as sending a reply e-mail or visiting

---

122 § 7702(2).
123 § 7702(17). The statute defines these as messages that facilitate, complete, or confirm a previously agreed upon commercial transaction; provide warranty, product recall, or product safety or security information with respect to a commercial product or service used or purchased by the e-mail recipient; provide notification concerning a change in the terms or features, notification of a change in recipient’s standing or status, account balance information, or any type of account information with respect to a subscription, membership, account, loan, or comparable ongoing commercial relationship; provide information directly related to an employment relationship or employee benefit plan in which the recipient is participating; or deliver goods or services that the recipient is entitled to receive under the terms of a prior transaction (e.g., software upgrades and updates).
124 See 16 C.F.R. § 316.2(m) (defining “sender” to include “when more than one person’s products, services, or Internet website are advertised or promoted in a single electronic mail message, each person within the Act’s definition will be deemed a sender . . .” unless certain requirements are met). Where multiple marketers have products, services, or websites advertised or promoted in the same commercial e-mail, they may designate as a single sender a person who (a) meets the definition of sender, (b) is identified in the “from” line as the sole sender of the message, and (c) complies with identified “core” provisions of the CAN-SPAM Act. Id.; 15 U.S.C. § 7706(f)(1) (civil penalties); 18 U.S.C. § 1037 (criminal penalties).
126 Senders of commercial e-mails that contain misleading header information, using “address harvesting” or “dictionary attacks,” or promoting sexual content have a separate set of requirements with which they must comply. For example, all e-mails containing sexual images or text that is otherwise subject to the Act must display the label “sexually explicit” in the e-mail subject line. 16 C.F.R. § 316.4. In addition, such messages must contain the equivalent of a “brown wrapper” displaying the physical address of the sender and describing the opt-out process, which must be opened separately from the e-mail itself. See id.
128 § 7704(a)(2).
129 § 7704(a)(3).
131 § 7704(a)(4)(A)(i).
a single web page, and it cannot be conditioned on the payment of a fee or providing information beyond the e-mail address or opt-out preference.  

- **Identify messages as advertisements.** Each commercial e-mail message must contain clear and conspicuous notice that the message is an advertisement or solicitation and that the recipient can opt out of receiving further commercial e-mails from the sender.

- **Contain the sender’s postal address within messages.** All commercial e-mail messages must include the sender’s valid physical postal address. A valid physical postal address is “the sender’s current street address, a Post Office box the sender has accurately registered with the United States Postal Service, or a private mailbox the sender has accurately registered with a commercial mail receiving agency that is established pursuant to United States Postal Service regulations.”

- **Maintain a black list.** Any entity that sends commercial e-mail messages must maintain a list of former recipients who have requested not to receive future commercial e-mails and honor such requests.

The FTC, other federal agencies, and state attorneys general divide enforcement responsibilities of the CAN-SPAM Act. Also, ISPs adversely affected by spamming may bring a civil action to enjoin further spamming and recover damages. Civil fines are $250 per e-mail, up to a maximum of $2 million per spamming event. Fines are subject to trebling for willful or knowing violations or for certain aggravated violations. Liability may be reduced if the defendant proves it established and implemented, with due care, commercially reasonable practices and procedures to prevent violations of the CAN-SPAM Act. Additionally, criminal penalties may apply, including prison sentences and forfeiture of computer equipment, for violations such as falsifying header information or sending commercial e-mails from multiple mail accounts registered under a false identity.

**Privacy of Financial Information**

The Gramm-Leach-Bliley Act (“GLB Act”) and the Fair Credit Reporting Act (“FCRA”) both regulate consumer information related to banking, credit, and insurance. While neither statute explicitly addresses Internet privacy issues, they apply to several industries heavily involved in doing business over the Internet. The GLB Act and the FCRA are among the most complex of federal statutes, and online businesses regularly dealing with financial information should consult an attorney with expertise in these statutes.

A. Gramm-Leach-Bliley Act

The GLB Act is extremely important to the many Internet businesses that offer consumers financing and bill-paying solutions or collect credit and financial profile information, as it imposes substantial privacy protection requirements for consumer information. The GLB Act created a three-headed regulatory regime under which federal banking and securities agencies oversee traditional banking and securities institutions, the individual states oversee insurance-related companies, and the FTC oversees all other businesses subject to constitutional limitations. In 2010, the Dodd-Frank Wall Street Financial Reform and Consumer Protection Act (the “Dodd-
Frank Act”) created an additional regulator, the Bureau of Consumer Financial Protection, which will also take an active role in enforcing the GLB Act against traditional banking and securities institutions.

The GLB Act defines “financial institution” extremely broadly. As defined in the GLB Act, “financial institutions” are those entities engaged in banking practices and certain “non-banking practices” under the Bank Holding Company Act. This definition brings within its scope businesses that might not otherwise view themselves as subject to financial regulations. For example, lawyers became concerned about their exposure to the GLB Act, and the American Bar Association (“ABA”) filed suit against the FTC in 2002. Joined by more than twenty-six other bar associations, the ABA challenged the FTC’s decision that lawyers who provide real estate, tax, estate planning, or other financial-related legal advice are subject to the privacy provisions of the GLB Act. The court found the FTC’s interpretation unwarranted and granted summary judgment to the ABA and its co-plaintiffs. The court determined that the plain language, the underlying purpose, and the legislative history of the GLB Act did not demonstrate a congressional intent to include attorneys in the definition of “financial institution.”

As a practical matter, the GLB Act is more of a “notice” statute than a significant restriction on the ability of financial institutions to share information. The GLB Act creates different notice obligations for financial institutions towards their “consumers” and “customers,” but it does not define either term. The GLB Act allows regulators to formulate their own definitions and rules to implement its objectives. For example, federal banking agencies and the Securities and Exchange Commission adopted the rule on Privacy of Consumer Financial Information, and federal banking agencies adopted a safeguards rule, which details the requirements of privacy notices. These rules also require each financial institution to develop a written “information security program” to identify how it currently uses personal information and the privacy risks associated with that use.

In July 2011, the Task Force on Consumer Compliance of the Federal Financial Institutions Examination Council, a group consisting of federal financial regulators, “adopted a voluntary model privacy notice form designed to make it easier for consumers to understand how financial institutions collect and share nonpublic personal information.” A financial institution that uses the model form falls within a “safe harbor” for compliance with the GLB Act requirements. Some of the terms of the model privacy notice form are

- Tell consumers they have a right to prevent some data sharing;
- Describe what data is being collected;
- Explain how the data will be shared;

---

146 Dodd-Frank Act § 1093 (amending 15 U.S.C. 6801 et seq.).
147 See 16 C.F.R. § 313.3(k).
149 Memorandum of the American Bar Association in Opposition to the FTCs Motion to Dismiss the Complaint at 19, New York State Bar Ass’n v. FTC, 276 F. Supp. 2d 110 (D.D.C. 2003); see American Bar Ass’n v. FTC, 430 F.3d 457 (D.C. Cir. 2005) (holding that the FTC had overstepped its authority in seeking to apply GLB Act privacy provisions to lawyers and law firms).
151 Id. at *3.
153 See, e.g. 17 C.F.R. pt. 248 (Securities and Exchange Commission Regulation S-P).
• List the reasons the data is shared;
• Describe the process to opt out of sharing;
• Provide contact information for consumers with questions.\textsuperscript{157}

While the preceding rules apply to financial institutions regulated by federal financial regulators, the FTC has also adopted rules to clarify and enforce the GLB Act. The FTC has attempted to clarify distinctions between consumers and customers within its rules. A consumer is an individual who provides nonpublic personal information\textsuperscript{158} to apply for or obtain a financial service for personal use,\textsuperscript{159} usually in an isolated transaction. An example of a financial service is when a financial institution evaluates information provided by an individual, like a credit or insurance application, and informs the individual of the outcome of the evaluation.\textsuperscript{160} That evaluation may be the sole financial product or service obtained.\textsuperscript{161}

The FTC evaluates both the substance and duration of the relationship to determine when a consumer becomes a customer, and the distinction rests on the particular facts and circumstances of the situation.\textsuperscript{162} A consumer becomes a customer when the consumer has agreed to form a continuing relationship with the institution, even if it is short term.\textsuperscript{163} An isolated transaction is not enough.\textsuperscript{164}

Different notice requirements apply to consumers and customers. When an individual becomes a consumer of a financial institution that will disclose (1) nonpublic personal information\textsuperscript{165} (2) to nonaffiliated third parties,\textsuperscript{166} the consumer is entitled to notice of the financial institution’s privacy policy and a reasonable opt-out method to prevent the disclosure.\textsuperscript{167} A consumer does not have these rights if the financial institution discloses only public personal information or discloses nonpublic personal information only to affiliates.\textsuperscript{168}

A consumer also does not have these rights if a financial institution discloses nonpublic personal information to a third party to (1) effect, administer, or enforce a transaction or service requested by the consumer or (2) process a financial product or service requested by the consumer.\textsuperscript{169} In other words, an express consent to the transaction is an implicit consent to share the necessary information to complete the transaction.

If a financial institution is required to provide notice of its privacy policy under the GLB Act, the privacy policy must contain certain information. The GLB Act states that a privacy policy must

• “Clearly and conspicuously” disclose to the consumer, in writing or electronic form, that nonpublic personal information may be disclosed to a third party;
• List the categories of nonpublic personal information collected by the financial institution and the categories of third parties to whom the information may be disclosed;
• Describe the third parties’ privacy policies and procedures;
• Specify the disclosure policies of nonpublic personal information regarding individuals who are no longer customers of the financial institution;

\textsuperscript{158} 65 Fed Reg. 33,650-51.
\textsuperscript{159} 16 C.F.R. § 313.3(e).
\textsuperscript{160} 65 Fed Reg. 33,651.
\textsuperscript{161} Id.
\textsuperscript{162} 65 Fed Reg. 33,652.
\textsuperscript{163} 16 C.F.R. § 313.3(h), (i); 65 Fed Reg. 33,652.
\textsuperscript{164} 65 Fed Reg. 33,652.
\textsuperscript{165} Nonpublic personal information means “personally identifiable financial information provided by a consumer to a financial institution resulting from any transaction with the consumer or any service performed for the consumer or otherwise obtained by the financial institution.” 15 U.S.C. § 6809(4). In addition, the information must not have been made public through government records or the media. 12 C.F.R. § 216.3(p).
\textsuperscript{166} A “nonaffiliated” third party is “any entity that is not an affiliate of, or related by common ownership or affiliated by corporate control with the financial institution.” 15 U.S.C. § 6809(5).
\textsuperscript{168} 65 Fed Reg. 33,652.
\textsuperscript{169} 15 U.S.C. § 6802(e).
• Describe the methods the financial institution uses to protect the confidentiality and security of consumers’ nonpublic personal information.\(^\text{170}\)  

In addition to providing a copy of the privacy policy to the consumer, the financial institution must provide the opportunity, before the disclosure of the information, to direct that the information not be disclosed to third parties. The financial institution must explain how the consumer can reasonably exercise this opt-out option.\(^\text{171}\) A consumer must be notified, but does not have a right to opt out, of disclosures of nonpublic personal information to third parties that perform business functions on behalf of the financial institution.\(^\text{172}\) The financial institution must have a contractual agreement with the third party requiring it to maintain the confidentiality of the information.\(^\text{173}\) These functions may include computer services, marketing, courier services, and other commonly outsourced services by companies.

Once a consumer becomes a customer, a financial institution has a new set of requirements under the GLB Act.\(^\text{174}\) A financial institution only needs to provide notice of its privacy policy to consumers when it intends to share nonpublic personal information with nonaffiliated third parties. However, when a consumer becomes a customer, the financial institution must provide notice of its privacy policy regardless of information sharing policies.\(^\text{175}\) The notice must be provided at the time a consumer becomes a customer and annually thereafter, as long as the customer remains a customer.\(^\text{176}\) The required contents of the privacy policy are described above.

The FTC has provided some clarity on how Internet-based financial institutions may provide the required notice. The FTC stated that initial notice may be made on a website if the user must acknowledge receipt as a step in the process of becoming a customer.\(^\text{177}\) Similarly, a financial institution may satisfy its annual notice requirement by posting the privacy policy on the financial institution’s website if the relationship with the customer occurs primarily through the website.\(^\text{178}\)

The GLB Act’s opt-out requirements were relatively novel and received substantial opposition from industry representatives. In response, Congress explicitly stated that the GLB Act does not preempt state financial privacy law.\(^\text{179}\) Therefore, states also have privacy laws that apply to financial institutions.

California’s Financial Information Privacy Act (known as “SB-1”) is one of several state privacy laws that do not strictly follow the GLB Act’s “opt-out” requirement. SB-1 requires financial institutions to obtain express opt-in consent from consumers before sharing personal financial information with nonaffiliated third parties that do not offer financial products or services.\(^\text{180}\) Likewise, in Illinois, a law requires express opt-in consent before banks can share personal financial information with nonaffiliated third parties.\(^\text{181}\) Both California and Illinois, however, arguably allow financial institutions to share information with nonaffiliated third parties “in connection with maintaining or servicing the customer’s account.”\(^\text{182}\) In Vermont, a statute provides that “a financial institution, its officers, employees, agents and directors shall not disclose to any person any financial information relating to a customer,”\(^\text{183}\) except when “authorized by the customer, provided the disclosure is limited to the scope and purpose

\(^\text{170}\) § 6803.  
\(^\text{171}\) § 6802(b)(1).  
\(^\text{172}\) § 6802(b)(2).  
\(^\text{173}\) § 6802(b)(2).  
\(^\text{174}\) An individual can become a consumer and customer at the same moment if he agrees to provides nonpublic personal information at the onset of a continuing relationship with the financial institution.  
\(^\text{176}\) § 6803.  
\(^\text{177}\) 65 Fed Reg. 33,665.  
\(^\text{178}\) Id.  
\(^\text{180}\) CAL. FIN. CODE § 4053(a), partially invalidated by American Bankers Ass’n v. Gould, 412 F.3d 1081, 1087 (9th Cir. 2005) (holding that the FCRA preempts SB1’s regulation of communication between affiliates).  
\(^\text{181}\) 205 ILL. COMP. STAT. 5/48.1(c).  
\(^\text{183}\) VT. STAT. ANN. Title 8, § 10203.
that the customer authorizes." § 10204(2).

§ 10204(2).

184 Several commentators have interpreted the Vermont statute as requiring express consent before sharing personal information with unaffiliated third parties.

B. Fair Credit Reporting Act

Information collection through consumer-credit-related activity is another area of active regulation that increasingly impacts Internet businesses. The FCRA is far more narrowly focused than the GLB Act, although the two laws complement each other. The GLB Act essentially incorporated an earlier version of the FCRA into its reporting requirements. For example, for a privacy policy to comply with the requirements of the GLB Act, it must include all disclosures required under the FCRA. In addition, as part of their GLB Act powers, the federal banking agencies and Federal Reserve Board may issue regulations and enforce the FCRA.

The FCRA applies to the communication of a “consumer report” by a “consumer reporting agency.” The “consumer report” is any information “bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for credit.” A “consumer reporting agency” is an entity that regularly generates or stores consumer reports.

The purpose of the FCRA is to “require that consumer reporting agencies adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information in accordance with the requirements of this title.” The statute regulates to whom a consumer reporting agency may furnish a credit report, the conditions that must be met before furnishing a credit report, and other compliance procedures.

The Fair and Accurate Credit Transactions Act (“FACTA”) added several new privacy protections for consumer credit information in 2003. As a result, a consumer has the right to receive one free credit report from each of the three nationwide consumer credit reporting companies (Equifax, Experian, and TransUnion) each year from the website “annualcreditreport.com.” Consumers can place alerts on their credit histories if they suspect identity theft and block fraudulent transactions resulting from identity theft from showing on their credit report. The FACTA amendments also require secure disposal of consumer information. Despite these new provisions, privacy advocates contend that the FACTA amendments favor the banking industry, because they limit consumers’ ability to stop financial institution affiliates from using their personal information for marketing purposes.

The FCRA represents the floor of consumers’ legal protections of their consumer reports, because, like the GLB Act, the FCRA contains an express preemption clause. Thus, states may enact laws controlling consumer reports and consumer reporting agencies if those laws or regulations are consistent with and stricter than the FCRA.

The FTC increased its FCRA enforcement efforts in 2012 with actions against Equifax, HireRight Solutions, and Spokeo. For example, Equifax Information Services LLC (“Equifax”) agreed to a consent order with the FTC.

184 § 10204(2).
186 § 6803 passim. A “consumer” is any individual person. § 1681a(c).
187 § 1681a(d)(1).
188 § 1681a(f).
189 § 1681.
190 § 1681b.
191 § 1681b.
192 § 1681c.
193 § 1681e.
197 See § 1681w.
198 § 1681t(a).
199 For a list of recent FTC activity related to the FCRA, see http://www.ftc.gov/opa/reporter/finance/creditreporting.shtml.
after its alleged violations of the FCRA. Equifax sells consumer reports to third parties as a consumer reporting agency. The FTC’s complaint alleged that over a period of two years Equifax sold more than 17,000 prescreened lists (i.e., lists of consumers who were late on their mortgage payments) to third parties that used the information for marketing products and services to the consumers on the lists, and Equifax allegedly had reason to believe the information was used for this impermissible purpose. In addition, Equifax provided access to such consumer report information through an online portal to third parties where Equifax allegedly “did not make reasonable efforts to verify the identity of these entities, and accordingly could not ensure that these entities would only use the lists for a permissible purpose.” The FTC concluded that Equifax’s alleged “failure to employ reasonable and appropriate measures to control access to the sensitive consumer financial information” violated the FCRA. Under the consent order, Equifax is prohibited from further violations of the FCRA and agreed to pay nearly $400,000 to the Commission.

The FCRA frequently impacts online businesses, particularly those that aggregate and monetize information through innovative techniques such as crowd sourcing. Many online businesses collect and verify user input as part of their platform, later providing that information to third parties. If such information is requested, provided, and used for credit reporting purposes, these entities may find themselves subject to FCRA requirements.

For example, in United States v. Spokeo, Inc., the Department of Justice, on behalf of the FTC, filed a complaint against online consumer profile provider Spokeo, Inc. (“Spokeo”). Spokeo allegedly collected consumer information from “hundreds of online and offline sources” and sold consumer profiles through paid subscriptions. According to the complaint, Spokeo entered into agreements with companies to use such profiles for human resources, background screening, and recruiting purposes. The Department of Justice alleged that the consumer profiles were consumer reports under the FCRA, and Spokeo violated the FCRA by not maintaining reasonable procedures to ensure that it furnished consumer reports to use for “permissible purposes” and failing to verify the identity of the prospective users of the consumer reports. Spokeo also allegedly did not use reasonable procedures to ensure the “maximum possible accuracy” of the information in the consumer reports or provide proper notice to the users of the consumer reports. As a result, Spokeo agreed to a civil penalty of $800,000 and is prohibited from future FCRA violations.

Compliance with FCRA requirements may be difficult, if not impossible, in situations where a website operator distributes aggregated information, because the information is gathered from public resources, and the website operator may make the information available free of charge with few direct controls. In some cases, compliance with specific notice and consent-related obligations of the FCRA could come into play. Thus, businesses should consider how the information they aggregate may be used and by whom.

Identity Theft

Identity theft is not a new problem. The Internet, however, has increased the incidence and harm of identity theft in the United States. To combat identity theft, Congress has implemented regulatory regimes through the GLB Act

202 Complaint at ¶ 11.
206 Complaint at ¶ 9.
207 Complaint at ¶ 10.
208 Complaint at ¶ 19, 23, 27, 31.
and FCRA. In addition, it enacted the Identity Theft and Assumption Deterrence Act (“ITADA”) of 1998,210 which criminalizes the creation of false, government-issued, identification documents. Federal regulators also adopted regulations to require financial institutions to develop identity theft prevention programs and to prevent the use of pretexting to obtain personal information by false pretenses.

A. Red Flags Rule

The FTC and several federal financial regulators211 jointly adopted the Red Flags Rule, under their FCRA authority as amended by FACTA, to help prevent identity theft.212 The Red Flags Rule requires creditors and financial institutions,213 as defined by the FCRA, that maintain “covered accounts”214 to develop and implement identity theft prevention programs215 designed to help detect and respond to so-called “red flags”216 indicating possible identity theft.217

Compliance with the Red Flag Rule requires a two-step, risk-based approach. First, an entity must determine whether it is a creditor or financial institution maintaining covered accounts. In the Red Flag Program Clarification Act of 2010, Congress defined creditors as an entity that (1) obtains or uses consumer reports in connection with a credit transaction; (2) furnishes information to consumer reporting agencies in connection with a credit transaction; or (3) advances funds to, or on behalf of, someone, except for funds for expenses incidental to a service provided by the creditor to that person.218 This definition narrowed the group of potential creditors by exempting doctors, lawyers, and other professionals. To be consistent with Congress’ change, in late 2012, the FTC narrowed the definition of “creditor” under the Red Flags Rule.219

Once an entity determines that it is a creditor or financial institution maintaining covered accounts, the second step is to design and implement a compliance program that is appropriate for its business operations. In all cases, the program must include procedures for the following: (a) identify red flags; (b) detect red flags; (c) respond to red

211 The financial regulators behind the Red Flags Rule are the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, the Office of Thrift Supervision, and the Board of Governors of the Federal Reserve System.
213 15 U.S.C. § 1681at(t) (“the term ‘financial institution’ means a State or National bank, a State or Federal savings and loan association, a mutual savings bank, a State or Federal credit union, or any other person that, directly or indirectly, holds a transaction account (as defined in section 461 (b) of title 12) belonging to a consumer.”). In response to the Red Flags Rule Clarification Act of 2010, in late 2012, the FTC narrowed the definition of “creditor” under the Red Flags Rule. It narrows the coverage to “creditors that regularly and in the ordinary course of business engage in at least one of the following three types of conduct: (1) obtain or use consumer reports directly or indirectly, in connection with a credit transaction; (2) furnish information to consumer reporting agencies in connection with a credit transaction; or (3) advance funds to or on behalf of a person, based on an obligation of the person to repay the funds or repayable from specific property pledged by or on behalf of the person.” Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act, 77 Fed. Reg. 72712, 72713 (2012), available at http://www.ftc.gov/os/2012/11/1211130redflagsrule.pdf.
214 16 C.F.R. § 681.1(b)(3) (“covered account means: (i) an account that a financial institution or creditor offers or maintains primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account; and (ii) any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial operational compliance, reputation, or litigation risks.”).
215 See § 681.1(d).
216 “Red flags” are “pattern[s], practice[s], or specific activit[ies] that indicates the possible existence of identity theft.” § 681.1(b)(9).
217 § 681.1(d).
flags; and (d) periodically review and update the program. Consistent with other information security best practices, an approved program must specify the person responsible for effectively implementing and administering the program. If the regulated entity lacks a board of directors, an appropriate senior-level employee may approve the program. Failure to comply with the Red Flag Rule may result in injunctive relief and civil penalties and could lead to claims under state consumer protection laws.

B. Pretexting

Pretexting is an effective identity theft strategy. It is the practice of obtaining a person’s personal information under false pretenses. Prior to 2006, the GLB Act was the primary federal law specifically limiting pretexting. The GLB Act prohibits pretexting to obtain personal financial information from either a financial institution or directly from a consumer. The GLB Act also prohibits using forged, counterfeit, lost, or stolen documents to acquire consumer information. In addition, the GLB Act prohibits the knowing solicitation of others to engage in pretexting. Federal regulators can enforce the GLB Act by seeking up to five years imprisonment for knowing violations and up to ten years for aggravated cases. The GLB Act has limitations, because it only applies to nonpublic, consumer information held by financial institutions and their business associates.

In 2006, Congress passed the Telephone Records and Privacy Protection Act (“TRPPA”) in reaction to a scandal involving pretexting at Hewlett-Packard. TRPPA expanded the scope of criminal pretexting to include fraudulently acquiring telephone records. HP’s troubles arose out of an internal investigation to determine the source of leaked confidential information from a member of HP’s Board of Directors. HP hired private investigators who allegedly engaged in pretexting to obtain copies of the phone records of the investigated individuals. After the public learned of the investigation and pretexting tactics, several law enforcement investigations ensued. Among them, the California Attorney General investigated whether independent investigators, at the direction of HP, used pretexting to obtain the telephone records of HP’s directors and members of the media. The California Attorney General alleged that HP’s internal investigation violated two California state laws: (1) California’s identity theft statute, prohibiting the use of someone else’s personal information to commit a crime, and (2) California’s computer crime laws, prohibiting unauthorized access to databases. HP ultimately settled with the California Attorney General, and the $14.5 million settlement will be used by California to create a Privacy and Piracy Fund to assist California state prosecutors investigate and prosecute consumer privacy and information piracy violations.

---

220 16 C.F.R. § 681.1(d).
221 § 681.1(e).
222 § 681.1(e).
223 § 681.1(b)(2).
225 § 6821(a)(3).
226 § 6821(b).
227 § 6822-23.
228 § 6801(a).
231 18 U.S.C. § 1039(a), (d)-(e) (imposing up to ten years in prison).
In reaction to the subsequent increase in public attention to pretexting, in 2007, the FCC amended its rules governing customer proprietary network information (“CPNI”) through a new CPNI order in *In re Implementation of the Telecommunications Act of 1996: Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information IP-Enabled Services.*\(^{235}\) CPNI is data collected by telecommunications carriers about customers’ phone calls.\(^{236}\) Through the 2007 CPNI Order, the FCC attempted to increase the security of personally identifiable data and CPNI, as well as discourage pretexting.\(^{237}\) To comply with the 2007 CPNI Order, a telecommunications carrier must password protect any online access to CPNI.\(^{238}\) Second, to protect against pretexting, the carrier may not disclose call detail information during a customer-initiated call, unless the customer provides the password.\(^{239}\) The carrier may not rely on “readily available biographical information” or “account information” as an alternative to requiring the password.\(^{240}\) Otherwise, the carrier may only release the call detail information by (1) sending the call records to an address of record, either postal or electronic; (2) calling the customer back at the telephone number of record; or (3) providing the call records at a store location upon proof of valid photo identification.\(^{241}\)

Third, the 2007 CPNI Order requires carriers to obtain consent prior to disclosing CPNI to independent contractors or joint venture partners for marketing purposes.\(^{242}\) Finally, the 2007 CPNI Order requires carriers to notify law enforcement whenever CPNI is disclosed through a security breach.\(^{243}\) The carrier must notify the U.S. Secret Service and FBI no later than seven business days after a “reasonable determination of a breach.”\(^{244}\) Seven days after notifying law enforcement, a carrier may notify the customer and disclose the breach publicly.\(^{245}\)

Pretexting continues to be a mechanism for compromising personal information. In 2009, a person was sentenced under TRPPA to twenty-one months in prison for serving Sprint/Nextel with a fake U.S. District Court civil subpoena to obtain telephone records of a Sprint/Nextel subscriber.\(^{246}\) Also in 2009, a defendant pled guilty to using a subscriber’s name and the last four digits of his Social Security number to obtain confidential phone records from T-Mobile.\(^{247}\)

### Children’s Privacy: COPPA, COPA, and the PROTECT Our Children Act

The privacy of children remains an increasingly important and ongoing legal concern for online businesses. Two applicable laws, the Children’s Online Privacy Protection Act (“COPPA”),\(^{248}\) and the Child Online Protection Act (“COPA”),\(^{249}\) are frequently confused but unrelated. COPPA focuses on privacy protection for children online, and the FTC has levied several substantial civil penalties as part of settlements in connection with alleged violations. The COPA, which focuses primarily on content regulation, has been struck down as unconstitutional by the courts. The PROTECT Our Children Act primarily focuses on child pornography.

#### A. Children’s Online Privacy Protection Act

---


236 *Id.* at 5.

237 *Id.* at 2-3.

238 *Id.* at 3.

239 *Id.* at 10-11.

240 *Id.* at 12-13, 15.

241 *Id.* at 10-11, 13, 16.

242 *Id.* at 22.

243 *Id.* at 19.

244 *Id.*

245 *Id.*


247 *Id.*


COPPA requires verifiable parental consent to collect information online from “children,” defined as individuals under the age of thirteen. The FTC’s COPPA rule requires a website operator to make reasonable efforts to obtain parental consent. The COPPA rule applies to all commercial websites that are directed to children or that knowingly collect personal information from children. The rule adopts a sliding scale approach to acceptable parental consent methods. If a website operator intends to share children’s personal information with third parties, it must use more reliable consent methods, such as a print-and-send consent form, a credit card transaction, or a toll free telephone number maintained by trained staff. If a website operator will use the children’s personal information for internal purposes only, it may implement an approach called “e-mail plus,” that the FTC considers less reliable. The method requires obtaining a parent's consent through e-mail and then taking an addition step to prove that the person providing the consent is in fact the parent. The FTC has clarified COPPA’s requirements by publishing a series of guides and FAQs. Many websites seek to manage COPPA-related risks by avoiding collection of children’s personal information and implementing mechanisms to limit usage based on age, such as age-neutral verification, a process whereby the website determines users’ ages without encouraging user deception.

At the end of 2012, the FTC issued its recent changes to the COPPA Rule, which will become effective July 1, 2013. Some of the changes include expanding the potential scope of liability such that websites or online service operators are liable for third parties collecting information on the websites or online services, such as “plug-ins,” and are responsible for providing parents with notice and obtaining verifiable parental consent. In addition, these third parties are obligated to comply with COPPA if they have actual knowledge that they directly collect personal information from users of a child-directed website or online service.

The FTC also amended the definition of “personal information” to include persistent identifiers that recognize a user over time and across different websites or online services. This may include cookies, IP addresses, and unique device identifiers. However, persistent identifiers are not considered “personal information” if they are only used for internal purposes. Further, “personal information,” now also includes: photographs, videos, and

251 § 6501(1).
253 16 C.F.R. § 312.5(b).
254 § 312.3.
255 § 312.5(b)(2).
256 § 312.5(b)(2).
257 § 312.5(b)(2).
259 An age-neutral screening system allows a user to freely enter his month, day, and year of birth. A website that only allows users to enter birth years making them 13 or older is not a neutral age-screening mechanism, because children cannot enter their correct age. Federal Trade Commission, Frequently Asked Questions about the Children's Online Privacy Protection Rule, http://www.ftc.gov/privacy/coppafaqs.shtm.
261 Final Rule and SBP at *17.
262 Id. at *26.
263 Id. at *37.
264 Id. at *154.
265 The new definition of "support for internal operations of [a] website or online service" includes those activities necessary to (i) maintain or analyze the functioning of the website or online service; (ii) perform network communications; (iii) authenticate users of, or personalize the content on, the website or online service; (iv) serve contextual advertising on the website or online service or cap the frequency of advertising; (v) protect the security or integrity of the user, website, or online service; (vi) ensure legal or regulatory compliance; or (vii) fulfill a request of a child as permitted by two exceptions to COPPA's verifiable parental consent requirements. Id. at *155. The FTC clarified specifically that “support for internal operations” does not include the collection of persistent identifiers used to track children over time and across sites or services, or to amass a
audio files that contain a child’s image or voice; screen or usernames that also function as “online contact information;” and geo-location information.266

Consistent with the FTC Privacy Report, the FTC simplified the content requirements of privacy notices provided to parents to make them shorter and simpler.267 Moreover, the FTC added new methods of obtaining verifiable parental consent, including: electronic scans of signed parental consent forms, videoconferencing, the use of electronic or online payment systems, and the use of government-issued identification checked against a database.268 The FTC also provided an application and approval process for entities to create other methods of obtaining verifiable parental consent.269

The updated COPPA Rule further requires website operators to take reasonable measures to release children’s personal information only to service providers and third parties that are capable of maintaining the confidentiality, security, and integrity of such information, and that provide assurances that they will maintain the information in such a manner.270

Finally, the updated COPPA Rule has data-retention and deletion provisions where operators must (1) retain children’s personal information for only as long as is reasonably necessary to fulfill the purpose for which the information was collected; and (ii) take reasonable measures to protect against unauthorized access to, or use of, the information in connection with its deletion.271

Failing to follow COPPA’s requirements can be costly. In 2004, the FTC imposed a $400,000 civil penalty against UMG Recordings for COPPA violations.272 The FTC alleged that UMG Recordings failed to (1) obtain verifiable parental consent before collecting extensive personal information from children on its music-related websites,273 (2) post a clear and complete privacy notice, and (3) provide parents notice of the websites’ intention to collect personal information from children.274 In 2006, the FTC brought an action against the operators of a social networking site, Xanga.com.275 Though Xanga’s user agreement prohibited children from joining, the website functionality permitted users to join who submitted a birth date indicating they were under thirteen years old.276 Xanga also failed to notify parents of its information practices and provide parents with the ability to control the information collected about their children.277 Xanga settled the FTC suit by paying a $1 million civil penalty and committing to implement compliance protocols.278 The FTC received a similar settlement in 2008 from Sony BMG Music.279 The FTC claimed that Sony collected, used, and disclosed personal information from at least 30,000

profile on an individual child user based on the collection of identifiers over time and across different websites in order to make decisions or draw insights about the child. Id. at *39.

266 Id. at *28-31, 40-46.
267 Id. at *54-60.
268 Id. at *160-61.
269 Id. at *81-85.
270 Id. at *95-96.
271 Id. at *96-99.
273 Id. ¶ 2.
276 Id.
277 Id.
278 Id.
children on its numerous music-related websites without giving proper notice about its collection, use, and disclosure practices.\(^\text{280}\)

In 2011, the FTC accepted a $50,000 settlement in its first COPPA action against a mobile application ("app") developer, W3 Innovations, LLC ("W3").\(^\text{281}\) W3 allegedly developed apps directed at girls under the age of thirteen.\(^\text{282}\) Some of the apps required children to enter their names to access features and allowed children to send e-mails to W3.\(^\text{283}\) Other apps provided links to an online blog, where children were encouraged to leave comments and required to enter an e-mail address to do so.\(^\text{284}\) The complaint stated that W3 collected over 30,000 children's e-mail addresses and collected personal information of over 600 app users who submitted blog comments.\(^\text{285}\) The FTC alleged two primary violations of COPPA. First, W3 failed to provide notice in their apps or direct notice to parents of "what information [they] collect from children, how they use such information, their disclosure practices, and all other required content."\(^\text{286}\) Second, W3C failed to obtain verifiable parental consent before collecting data from children.\(^\text{287}\)

B. Child Online Protection Act

COPA was, essentially, an online-decency act. COPA required entities "mak[ing] any communication for commercial purposes that is available to any minor and that includes any material that is harmful to minors"\(^\text{288}\) to restrict access to such material to persons over seventeen years of age.\(^\text{289}\) COPA exempted ISPs from these requirements\(^\text{290}\) and provided an affirmative defense to entities that attempted to restrict access to the material by methods such as requiring the use of a verified credit card.\(^\text{291}\) Privacy advocates argued that COPA violated the First Amendment because it essentially required individuals seeking to access material deemed "harmful to minors" to identify themselves.\(^\text{292}\) After a series of court challenges, the Third Circuit upheld a permanent injunction preventing the federal government from enforcing COPA in the 2008 case American Civil Liberties Union v. Mukasey.\(^\text{293}\) The Supreme Court denied the petition for writ of certiorari in 2009,\(^\text{294}\) effectively bringing an end to COPA as a consideration for most businesses.

C. PROTECT Our Children Act

The PROTECT Our Children Act of 2008 (the "PROTECT Act")\(^\text{295}\) requires ISPs to report child pornography to the National Center for Missing and Exploited Children ("NCMEC").\(^\text{296}\) The NCMEC is a private, nonprofit

\(^{280}\) Id.


\(^{283}\) Id. ¶ 12.

\(^{284}\) Id. ¶¶ 14-15.

\(^{285}\) Id. ¶ 20.

\(^{286}\) Id. ¶¶ 23-24.

\(^{287}\) Id. ¶ 25.


\(^{289}\) § 231(d)(1)(A).

\(^{290}\) See § 231(b).

\(^{291}\) See § 231(c)(1).

\(^{292}\) See Am. Civil Liberties Union v. Reno, 31 F. Supp. 2d 473, 480 n.2, 491 (E.D. Pa. 1999); see also Ashcroft v. Am. Civil Liberties Union, 535 U.S. 564, 571 n.5 (2002) (noting the anonymity argument, but as not relevant to legal issue under review (citation omitted)).


\(^{296}\) 18 U.S.C. § 2258A(a). The reporting requirements include misleading domain names that involves child pornography. § 2258A(a)(2)(A) (incorporating "an apparent violation of" 18 U.S.C. 2252B involving child pornography). Section 2252B prohibits the knowing use of misleading domain names that trick people into viewing obscene material or trick children into viewing “material that is harmful to minors.” § 2252B(a), (b).
organization that Congress created to serve as a national clearing house for information on missing and exploited children.\textsuperscript{297} An ISP that has knowledge of child pornography and fails to report it is subject to fines up to $150,000, and up to $300,000 for subsequent failures to report.\textsuperscript{298} The PROTECT Act allows for civil causes of action against ISPs that intentionally, recklessly, or with actual malice failed to report the material.\textsuperscript{299} Like COPA, the PROTECT Act faced constitutional challenges. However, in United States v. Cameron,\textsuperscript{300} the trial court held that ISPs are acting as citizen enforcers under the PROTECT Act, and, therefore, Fourth Amendment protections did not apply when Yahoo! gave evidence to law enforcement.\textsuperscript{301} Many online services that enable user-generated-content frequently review and take steps to conform their conduct with the PROTECT ACT in connection with certain types of content. Balancing the privacy interests of users with related legal exposure for possessing content subject to the PROTECT ACT is an increasingly common issue confronting online businesses.

**Personal Health Information: Health Insurance Portability and Accountability Act**

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA")\textsuperscript{302} greatly affected the use and storage of health information in the United States. HIPAA attempted to simplify and standardize health care administration by creating standards for the exchange of electronic health records.\textsuperscript{303}

The Department of Health and Human Services ("HHS") adopted the HIPAA Privacy Rule to protect the privacy of these electronic health records.\textsuperscript{304} The HIPAA Privacy Rule covers "protected health information" ("PHI") maintained, accessed, used, or disclosed by covered entities.\textsuperscript{305} PHI includes any individually identifiable health information.\textsuperscript{306} PHI does not include information that is "de-identified."\textsuperscript{307} Information is de-identified if it does not include data like a person’s name, account number, or zip code, or an expert has determined that the data is incapable of "re-identification."\textsuperscript{308}

A "covered entity" is a health plan, a health care clearinghouse, or a health care provider that transmits electronic health information for typical health care related reasons.\textsuperscript{309} Beginning in 2009, the HIPAA Privacy Rule also

\textsuperscript{298} 18 U.S.C. § 2258A(e).
\textsuperscript{299} § 22588B(b).
\textsuperscript{300} United States v. Cameron , 729 F. Supp. 2d 418 (D. Me. 2010).
\textsuperscript{301} Cameron , 729 F. Supp. 2d at 421-24.
\textsuperscript{303} See id; 42 U.S.C. § 1320d-2 (note).
\textsuperscript{305} 45 C.F.R. § 160.102.
\textsuperscript{306} § 160.103. “Health information” includes any information that is created or received by a covered entity, school or university, public health authority, employer, or life insurer, or healthcare clearinghouse; which relates to the past, present, or future health of an individual, the provision of healthcare to an individual, or payment for the provision of healthcare to an individual. § 160.103.
\textsuperscript{307} See § 164.514(a) (“Health information that does not identify an individual . . . is not individually identifiable health information.”); § 160.103 (“Protected health information means individually identifiable health information . . . ”).
\textsuperscript{308} § 164.514(b)(1), (2).
\textsuperscript{309} §§ 160.102(a); 164.104. These reasons include health care claims, payment, benefit coordination, enrollment, and eligibility inquiries. § 160.103.
applies to “business associates” of covered entities.310 “Business associates” are entities that perform for covered entities business functions that involve the access, use, or disclosure of PHI.311

The HIPAA Privacy Rule provides individuals with the following seven rights concerning their PHI:

- **Notice**: An individual has a right to receive adequate, written notice of his rights under HIPAA and the regulated entity’s uses and disclosures of PHI.312 This notice must be written in “plain English” and contain contact and complaint-filing information.313

- **Access**: An individual normally has a right to obtain and inspect a copy of his PHI.314

- **Amendment**: An individual usually has a right to amend or correct his PHI.315

- **Consent**: Regulated entities must obtain an individual’s written consent before using or disclosing PHI.316 Limited exceptions exist. For example, regulated entities may use or disclose PHI for emergency treatment purposes without consent so long as consent is obtained as soon as practicable.317 An enhanced form of consent, “authorization,” is required for some disclosures. Authorizations must specifically and meaningfully describe the information to be used or disclosed, describe the parties that will exchange the information, explain the purpose of the use or disclosure, and state the expiration date of the authorization. Authorization is generally required for uses and disclosures that unrelated to treatment, payment, or health care operations.318

- **Request for Privacy**: An individual has a right to require a regulated entity to use his PHI only when necessary for treatment, payment, or health care operations.319

- **Accounting**: An individual has a right to receive an accounting of PHI disclosures within the previous six years, including the identification of entities to which they were made.320

- **Minimum Necessary**: There is a general requirement that the use and disclosure of PHI be the minimum necessary for the purpose of the use or disclosure.321 Again, certain exceptions apply.322

---


311 45 C.F.R. § 160.103. Only entities that require routine access to PHI to perform data transmission services are considered business associates. See Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the HITECH Act, 75 Fed. Reg. 40,868, 40,873 (proposed July 14, 2010) (to be codified at 45 C.F.R. § 160.102). Thus, data transmission service providers that act only as “mere conduits” for movement of PHI, with only “random or infrequent” access to that PHI are not business associates. Id. Examples of entities the HHS considers to be such “mere conduits” are the United States Postal Service and “certain private couriers and their electronic equivalent.” 45 C.F.R. § 160.103 (citing http://www.hhs.gov/ocr/privacy/hipaa/faq/providers/business/245.html).

312 45 C.F.R. § 164.520(a)(1). In this section, this article will use the term regulated entity to include both covered entities and their business associates.

313 § 164.520(b). The notice must also say, “THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.” § 164.520(B)(1)(i).

314 § 164.524(a)(1). Access limitations include psychotherapy notes, information compiled in anticipation of a trial, and health information subject to the Clinical Laboratory Improvements Amendments of 1988. § 164.524(a)(1).

315 § 164.526(a). A regulated entity may deny an amendment if the record is “accurate and complete”; if the regulated entity did not create the record; if the record in question is not part of the requested set; or if the record is one that is not accessible under 45 C.F.R. § 164.524. § 164.526(a).

316 § 164.506(a)(1).

317 § 164.510(a)(3).

318 See § 164.508 (setting out situations in which authorization is required).

319 § 164.522(a)(1).

320 § 164.528(a)(1).

321 § 164.502(b)(1).

322 See § 164.502(b)(2).
HIPAA requires regulated entities, when transmitting information, to maintain reasonable safeguards to protect data. These reasonable safeguards must “ensure the integrity and confidentiality” of data and protect against “any reasonably anticipated” threats, hazards, unauthorized uses, or disclosures.

In 2009, the HITECH Act amended HIPAA to provide additional protections. In addition to extending the HIPAA to include business associates, it created additional notice requirements for PHI data breaches and strengthened the penalties for failing to comply.

The HITECH Act also created a tiered civil penalty structure that limits HHS’s discretion when assessing penalties. The penalties remain significant and vary based on culpability. Penalties start at $100 per violation, with an annual cap of $25,000 for identical violations. Penalties can reach $50,000 for each violation, with a $1.5 million annual cap for identical violations. A HIPAA violation may be resolved without a civil fine if it was not the result of willful neglect and was corrected within thirty days of discovery. Moreover, even if HHS chooses not to impose a fine, state attorneys general may bring civil actions for damages. Thus, any HIPAA violation carries with it both the risk of a large fine, damages compensation to victims, and additional litigation costs.

HHS has increased its enforcement activity for violations of the HIPAA Security Rule. The HIPAA Security Rule imposes strict security requirements on covered entities that collect, use, and disclose electronic PHI (e-PHI) and on business associates providing services for them. These entities must maintain reasonable and appropriate administrative, technical, and physical safeguards. The HIPAA Security Rule is flexible and scalable so that the level of appropriate safeguards is determined by the specific environment based on the nature of the entity’s business and its size and resources and the potential risks to the e-PHI.

HHS reached four settlements in 2012 totally almost $5 million. For example, in September 2012, HHS alleged several violations of the HIPAA Security Rule when Massachusetts Eye and Ear Infirmary and Massachusetts Eye and Ear Associates, Inc. (collectively "MEEI") had an unencrypted laptop containing e-PHI stolen. In addition to the $1.5 million settlement amount, MEEI agreed to comply with a corrective action plan (CAP). The CAP requires independent monitoring and annual written compliance reports by MEEI to HHS.

Regulators continue to impose new requirements on entities subject to HIPAA. On May 27, 2011, HHS released a Notice of Proposed Rulemaking regarding the HIPAA Privacy Rule’s accounting provision. The proposed revision to the Privacy Rule sets forth two separate individual rights: (1) the right to an access report, and (2) a right to an accounting of disclosures. The access report would include summary information from the prior three years.

326 See 42 U.S.C. § 17932. Covered entities must notify affected individuals within 60 days of a data breach. § 17932(d)(1). They must also notify HHS and the media if the breach affects more than 500 people. § 17932(e)(2). If a breach affects data possessed by a business associate, it must notify the covered entity for which it is providing the service. § 17932(b).
327 See § 1320d-5(a)(3).
328 See § 1320d-5(a)(1).
332 See § 1320d-5(d).
333 The Security Rule is located at 45 CFR Part 160 and Subparts A and C of Part 164.
335 U.S. Department of Health & Human Services, Massachusetts provider settles HIPAA case for $1.5 million, http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/meei-agreement.html
337 Id. at Appendix A.
339 Id. at 31428-29.
about anyone who has accessed electronic PHI in a designated record set held by a covered entity or business associate. The right to an accounting would allow a person to obtain more detailed information about a particular disclosure of PHI held in any format. The new rights would broaden the accounting rule, as the access report would include both internal employees’ and business associates’ access to electronic PHI. In September 2011, HHS issued a model privacy notice that can be used voluntarily by companies that hold personal health records.

In November 2012, HHS issued its Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule ("De-identification Guidance"). The De-identification Guidance provided two methods to de-identify PHI in accordance with the HIPAA Privacy Rule: expert determination and Safe Harbor. As mentioned above, properly de-identified information is not PHI covered by HIPAA when it does not identify an individual and if the covered entity has no reasonable basis to believe it can be used to identify an individual.

The first method described by HHS is the expert determination method where a person with appropriate knowledge and experience in de-identification applies generally accepted statistical and scientific principles for de-identifying information to the information and determines that the risk is very small that the information could be used to identify an individual and the expert documents the methods and results of the analysis. HHS did not place an explicit numerical level of acceptable risk in identification, as the risk depends on different data sets and environments. HHS recommends the following principles be used to assess the identifiability of health information: replicability, data source availability, and distinguishability.

The second method of de-identification requires the removal of a certain data elements, including: patient name, geographic information, dates, contact information, social security numbers and other identification numbers, biometric identifiers, and full-face photographs. In addition, the covered entity may not have actual knowledge that the remaining information could be used alone or in combination with other information to identify an individual.

HIPAA preempts contrary provisions of state law, but states are allowed to adopt more protective regulations. For example, the California Confidentiality of Medical Information Act ("CMIA") is similar to HIPAA and likely covers more entities than the HIPAA. In addition, the CMIA has stricter timing requirements of when state-complying data breach notices must be sent, but the notice document requires less information than HIPAA requires. A final important difference is that the CMIA gives California residents private rights of action. Texas enacted the Texas Medical Privacy Act ("TMPA") to protect its citizens. Similar to the California law, the TMPA likely covers more entities than the HIPAA.

---

340 Id.
341 Id. at 31429.
342 Id.
345 Id. at 4.
346 45 C.F.R. § 164.514(a).
347 § 164.514(b).
348 Id.
349 Id. at 13-14.
350 45 C.F.R. § 164.514(b).
351 § 164.514(b).
352 See CAL. CIV. CODE § 56.05 - 06.
353 CAL. HEALTH & SAFETY CODE § 1280.15(b).
354 TEX. HEALTH & SAFETY CODE ANN. § 181.001(b)(1)(A)-(D).
Telephone Consumer Protection Act

The Telephone Consumer Protection Act of 1991 ("TCPA") banned many commercial solicitation calls to residences made without prior consent. In particular, a commercial solicitor may not "make any call . . . using any automatic telephone dialing system or an artificial or prerecorded voice" to emergency phone lines, pagers, or cell phones, or make a call for which a charge is made to the calling party. The TCPA placed enforcement authority with the FCC, and it also granted states and individuals a private right of action prescribing $500 in damages for each violation and possible trebling for willful or knowing violations. Therefore, damages can be substantial.

The TCPA does not define the term "call," which has led to litigation, particularly with regard to whether it includes text messages. The FCC has defined the term to include text messages, and courts have agreed. In the 2009 case of Satterfield v. Simon & Schuster, Inc., the Ninth Circuit found the FCC's interpretation of "call" reasonable, because text messaging is a communication method between telephones, and Congress's purpose with the TCPA was to limit communications to "protect the privacy interests of residential telephone subscribers." Potentially exposed to $90 million in damages, in 2010, Simon & Schuster agreed to settle this class action case for $10 million, entitling plaintiffs to $175 per text message received. Numerous consumer class actions have been filed alleging TCPA violations in connection with new online services that utilize text messaging and alleging privacy violations from unwanted text messages. The FCC has a pending proceeding where commenters have alleged that Congress never intended the TCPA to apply to such services.

Cable Communications Act

The Cable Communications Policy Act ensures that cable operators consider the interests of subscribers, including the privacy interests in their personally identifiable information ("PII"). Under the Cable Communications Policy Act, PII is defined as non-aggregate data that identifies a particular individual. A subpart of the Cable Communications Act, known as the Cable TV Privacy Act ("TV Act"), generally prohibits cable operators from collecting and disclosing PII without consent, unless the collection is necessary to conduct legitimate business related to cable service or pursuant to a court order if the subscriber has prior notice. Additionally, cable operators may disclose subscriber name and address information if the operator has allowed the subscriber an opportunity to opt out of such disclosure and the information does not reveal the subscriber's viewing habits or transactions with the cable operator.
legitimate cable-related business and to detect unauthorized cable access. The TV Act places a duty on cable operators to prevent unauthorized, third-party access to PII. Additionally, cable operators must notify subscribers of what PII is collected, how long it is stored, and if it is disclosed to third parties.

Courts have refused to apply the TV Act requirements to ISPs in their capacity as ISPs, even when the ISP is also a cable provider and is streaming video over its Internet service. For example, in Klimas v. Comcast Cable Communications, Inc., the Sixth Circuit dismissed a class action lawsuit brought under the TV Act against Comcast. The plaintiffs claimed that Comcast had violated the TV Act by collecting the IP addresses of subscribers to Comcast’s Internet service. The Klimas court held, however, that “cable service” under the TV Act does not include broadband internet service, even when provided by a “cable operator.” Despite the result of this case, cable companies, which also provide high-speed Internet service, generally follow the restrictions for all of its data, because consumers do not understand the limits of the TV Act and assume it governs all of the data the cable company collects about them. Other emerging service providers have also looked to the TV Act as a benchmark for developing best practices and managing privacy-related risks.

**White House’s Privacy Framework**

The White House proposed its own privacy framework for consumer privacy with four approaches:

- a proposed Consumer Privacy Bill of Rights;
- a “multistakeholder process” by which government, industry, advocates, academics, and others will develop enforceable codes of conduct to implement that Bill of Rights;
- legislative action to give the Federal Trade Commission (FTC) a statutory basis to enforce the Bill of Rights; and
- increased cooperation and coordination with foreign countries on privacy issues.

The Consumer Bill of Rights describes seven data privacy principles: individual control, transparency (e.g., privacy notices), respect for context (e.g., relationship with the consumer), security, access and accuracy, focused

---

368 § 551(b)(2).
369 § 551(b)(1), (c)(1). Cable operators may disclose collected PII if necessary to conduct legitimate business related to cable service or pursuant to a court order if the subscriber has prior notice. § 551(c)(2)(A)-(B). Additionally, cable operators may disclose subscriber name and address information if the operator has allowed the subscriber an opportunity to opt out of such disclosure and the information does not reveal the subscriber’s viewing habits or transactions with the cable operator. § 551(c)(2)(C); § 551(c)(1) (placing the duty on cable operators).
370 See § 551(a)(1). Additionally, cable providers must inform subscribers about how subscribers may access this data and the requirements under the Cable TV Privacy Act. § 551(a)(1)(C)-(E).
371 See Klimas v. Comcast Cable Communications, Inc., 465 F.3d 271, 275-76 (6th Cir. 2006); see also In re Application of the United States for an Order Pursuant to 18 U.S.C. § 2703(D), 157 F. Supp. 2d 286, 290-92 (S.D.N.Y. 2001) (discussing legislative history indicating that Congress did not intend Cable TV Privacy Act requirements to apply in situations beyond the provision of cable services); Kimberlite Corp. v. Does 1-20, No. C08-2147 TEH, slip op. at 4 (N.D. Cal. June 2, 2008) (noting that there is legal authority for the proposition that an ISP does not provide cable service under the Cable TV Privacy Act (citing Klimas, 465 F.3d at 279-80, AT&T Corp. v. City of Portland, 216 F.3d 871, 876-77 (9th Cir. 2000))).
372 Klimas, 465 F.3d 271.
373 Id. at 273.
374 Id. at 274.
375 Id. at 280. The court’s reasoning was in part based on a series of FCC decisions and relevant federal case law. Id. (citing National Cable & Telecommunications Association v. Brand X Internet Services, 545 U.S. 967 (2005); In re Inquiry Concerning High-Speed Access to the Internet Over Cable and Other Facilities, 15 F.C.C.R. 19287 (2000); In re Inquiry Concerning High-Speed Access to the Internet Over Cable and Other Facilities, 17 F.C.C.R. 4798 (2002)). In this series of decisions, with the Supreme Court’s eventual approval, the FCC distinguished cable Internet services from the general category of telecommunications services, under which cable TV service falls. See National Cable & Telecommunications Association v. Brand X Internet Services, 545 U.S. 967 (2005); In re Inquiry Concerning High-Speed Access to the Internet Over Cable and Other Facilities, 15 F.C.C.R. 19287 (2000); In re Inquiry Concerning High-Speed Access to the Internet Over Cable and Other Facilities, 17 F.C.C.R. 4798 (2002).
collection (including proper disposal), and accountability (e.g., audits). The White House also supported the development and enforcement of sector-specific codes of conduct. As a first step, the National Telecommunications & Information Administration held a series of stakeholder meetings throughout 2012 and continuing into 2013, to develop a code of conduct regarding mobile app transparency. The impact of this privacy framework remains to be seen.

Other Federal Statutes

In addition to the foregoing laws, the following federal laws impact the protection of personal privacy in specific areas:

- Electronic Funds Transfer Act, governing financial records;\(^{377}\)
- Privacy Act of 1974, regarding government use of personal data;\(^{378}\)
- National Information Infrastructure Protection Act of 1996;\(^{379}\)
- Title III of the Omnibus Crime Control and Safe Streets Act of 1968,\(^{380}\) regulating law enforcement’s ability to perform wiretapping on telephone and telegraph lines;
- Communications Assistance for Law Enforcement Act,\(^{381}\) requiring telecommunications carriers to enable their networks for government surveillance in a manner specified by technical standards issued by the Federal Communications Commission, with the goal of replicating law enforcement’s telephone wiretapping capability on other electronic media;
- Driver’s Privacy Protection Act;\(^{382}\)
- Right to Financial Privacy Act;\(^{383}\)
- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act);\(^{384}\)
- Video Privacy Protection Act;\(^{385}\) and
- E-Government Act of 2002, requiring federal agencies to implement certain policies concerning their collection of personal information from agency websites, among other things.\(^{386}\)

The federal laws listed above frequently impact very specific behaviors or industry segments. While this article does not devote significant attention to them, they exemplify the breadth of U.S. laws impacting privacy issues.

KEY STATE PRIVACY LAWS

In addition to federal law, state law also protects citizens against invasions of privacy. Comparable to federal law, state privacy protection arises from state constitutions and statutes. States also protect common law rights, but little common law has developed to protect against modern privacy invasions. This section will identify some examples of privacy law arising from state constitutions, state statutes, and the common law. A state-by-state analysis of privacy laws is beyond the scope of this article; however, practitioners preparing to bring a claim asserting privacy rights should refer to state laws for additional sources of protection for their clients.


\(^{378}\) 5 U.S.C. § 552(a). The Office of National Drug Control Policy ran afoul of the Privacy Act in June 2000 when the Office’s website, in violation of the Act and the website’s own privacy policy, secretly collected information on users’ searches via cookies. The incident prompted a White House directive that all agency website privacy policies be reexamined.

\(^{379}\) Pub. Law 104-294.


\(^{381}\) 47 U.S.C. §§ 1001-1010.

\(^{382}\) 18 U.S.C. § 2721.


State Constitutions

Ten states have granted a constitutional right to privacy.387 Most of those states explicitly declared a right to privacy, but other states have implied the right using language that more closely resembles the Fourth Amendment.388 Regardless, many state courts use Fourth Amendment jurisprudence to interpret their state constitution.390 Therefore, protection from the search and seizure of electronic communications under state constitutional law does not differ substantially from the protections under the federal Constitution. Notably, of the states explicitly recognizing a constitutional right to privacy for public employees, only California extends such protection to private employees.391 To date, however, California courts have refused to afford private-sector employees a constitutional right of privacy in workplace e-mail communications.392

“Spam”

The federal CAN-SPAM Act preempts state laws that expressly regulate the transmission of commercial e-mail, except where such laws target false or deceptive e-mail content.393 Therefore, while many states have anti-spam laws, they tend to apply in few cases. Thirty-nine states currently have anti-spam statutes, including California, Texas, Florida, and Illinois.394 These four states provide representative samples of the remaining states. Their anti-spam statutes prohibit false or misleading information in routing information of commercial e-mails.395 California, Illinois, and Texas provide a private right of action for any person who suffers damage from spam.396 The costs of violating the anti-spam laws can be significant. California provides for damages of $1,000 per prohibited e-mail, with a cap of $1 million.397 Texas and Illinois allows for damages of the lesser of $10 per prohibited e-mail or $25,000 per day, with no cap.398 Due to the likelihood that bulk commercial e-mail will go to residents of every state, businesses involved in solicitation by bulk e-mail should carefully consider all state anti-spam laws.

388 See, e.g., ALASKA Const. art. I, § 22 (“The right of the people to privacy is recognized and shall not be infringed.”); MONT. Const. art II, § 10 (“The right of individual privacy is essential to the well-being of a free society and shall not be infringed without the showing of a compelling state interest.”).
391 Id. at 644 (“[T]he Privacy Initiative in article I, section 1 of the California Constitution creates a right of action against private as well as government entities.”).
392 See Holmes v. Petrovich Dev. Co., 119 Cal. Rptr. 3d 878, 898 (Cal. Ct. App. 2011) (“Here, we are not concerned with a potential Fourth Amendment violation because Holmes was not a government employee.”).
395 CAL. BUS. & PROF. CODE §§ 17529-17529.9, 17538.45.
396 TEX. BUS. & COM. CODE ANN. §§ 321.001-.114.
397 FLA. STAT. §§ 668.60-.610.
398 815 ILL. COMP. STAT. §§ 511/1 to 511/15.
399 CAL. BUS. & PROF. CODE § 17529.5(a)(2); FLA. STAT. § 668.603(1)(b); 815 ILL. COMP. STAT. § 511/10(a)(i); TEX. BUS. & COM. CODE ANN. § 321.104(b)(1).
400 CAL. BUS. & PROF. CODE § 17529.5(b)(1)(A); 815 ILL. COMP. STAT. § 511/10(c); TEX. BUS. & COM. CODE ANN. § 321.104(a). Florida’s statute, however, limits civil actions to telecommunications service providers. See FLA. STAT. § 668.606(1).
402 815 ILL. COMP. STAT. § 511/10(c); TEX. BUS. & COM. CODE ANN. § 321.105(a).
Identity Theft

All fifty states have statutes targeting identity theft or impersonation.403 These laws criminalize the practice of identity theft, create private rights of action for damages, and facilitate victims’ ability to repair their legal or credit histories. After several well-publicized data breaches where thousands of credit cards were stolen, states enacted data breach notification statutes, which are discussed below.

Privacy Policies

California was the first state to require commercial website operators to post a privacy policy when it passed the California Online Privacy Protection Act of 2003 (“OPPA”).404 The OPPA applies to website operators that collect PII about California residents who use their website or online service.405 The OPPA requires that privacy policies (1) be conspicuous, (2) specify the effective date, (3) explain the user notification process when the policy is amended, and (4) describe what information the website collects and how it is collected.406 The OPPA does not have an enforcement clause, and commentators have speculated that remedies are available under California’s Unfair Competition Law.407

Data Breach Notification

Compliance with state breach notification requirements is a significant challenge for many businesses, because notification requirements vary by state. California was also the first state to require entities conducting business in the state to promptly disclose to affected people a security breach resulting in the acquisition of unencrypted personal information by an unauthorized person (“California’s breach notification statute”).408 California’s breach notification statute applies to “any person or business that conducts business in California,” if the entity possesses “computerized . . . personal information.”409 If a “breach of the security system”410 occurs, the business must inform affected people “in the most expedient time possible and without unreasonable delay”411 using a notification that conforms to the statutory requirements.412 A business may delay such notice if a law enforcement agency determines that immediate notification will impede an investigation, but the business must notify the affected people as soon as the law enforcement delay ends.413 Notice can be sent by mail or electronically.414 A notice is compliant if it conforms to the business’s existing “information security policy.”415 Consequently, businesses may wish to specify their information security policy in their privacy policies. Such a provision could assure businesses that their notification method complies with California’s breach notification statute. Additionally, California deems HIPAA-covered entities that comply with Section 13402(f) of the HITECH Act416 as compliant with the California’s notice

---

403 Nat’l Conference of State Legislatures, Identity Theft State Statutes, NCLS.ORG, (Aug. 31, 2010), http://www.ncsl.org/?tabid=12538 (containing a list of state and territory statutes, including citation, title, and information on criminal penalties and restitution).


405 CAL. BUS. & PROF. CODE § 22575(a).

406 § 22575(b).


409 CAL. CIV. CODE § 1798.82(a).

410 § 1798.82(f). A breach of the security of the system is defined any unauthorized acquisition of personal data, not just credit card data theft. Id.

411 § 1798.82(a).

412 § 1798.82(b). Security breach notifications must be written in plain language and must include the name and contact information of the reporting entity, a list of information believe to be exposed, the date of the breach insofar as it is possible to determine, whether notification was delayed per law enforcement request, and a general description of the incident. § 1798.82(b).

413 § 1798.82(a), (c).

414 § 1798.82(j).

415 § 1798.82(k). The information security policy must be “consistent with the timing requirements of this part . . . .” § 1798.82(k).

requirements.\footnote{CAL. CIV. CODE § 1798.82(e).} Failing to provide the required breach notice may subject a business to civil damages and
injunctive relief.\footnote{§ 1798.84.}

Recent amendments to the California’s breach notification statute specified new requirements for California
breach notifications, including that notifications must (1) be in plain language, (2) identify and provide contact
information of the entity sending the notification, and (3) generally describe the compromised information.\footnote{2011 Cal. Legis. Serv. Ch. 197 (S.B. 24), § 2 (WEST) (amending CAL. CIV. CODE § 1798.82).}
Several states now have similar laws.\footnote{See, e.g., ARIZ. REV. STAT. ANN. § 44-7501 (enacted 2007); ARK. CODE ANN. § 4-110-105 (enacted 2005); CONN. GEN. STAT. § 36a-701b (enacted 2006); GA. CODE ANN., § 10-1-912 (enacted 2005); MASS. GEN. LAWS ch. 93H, § 3 (enacted 2007);tex. bus. & com. code ann. § 521.053 (enacted 2009).}

Massachusetts’s notice statute, the Massachusetts Data Breach Notification Law,\footnote{2011 Cal. Legis. Serv. Ch. 197 (S.B. 24), § 2 (WEST) (amending CAL. CIV. CODE § 1798.82(f)).} is similar to California’s. It applies to a business or government agency that maintains, stores, owns, or licenses “personal information about a
resident of the commonwealth.”\footnote{§ 3.} If a breach occurs, the business “shall provide notice, as soon as practicable and
without unreasonable delay” upon learning of the breach.\footnote{§ 3.} If a business owns or licenses the compromised data,
notice must be given to the Attorney General, Office of Consumer Affairs, and Massachusetts residents whose data
was compromised.\footnote{§ 4.} “Notice may be delayed if a law enforcement agency determines that provision of such notice
may impede a criminal investigation.”\footnote{§ 1.} Notice can be sent by mail, electronically, or by publication for large data
breaches that would require costly individual notice.\footnote{§ 1.}

Massachusetts goes far beyond California and other states with its privacy requirements, because it (1) prescribes
that businesses take preventive measures as well as post-breach responses and (2) applies to government agencies as
well as private businesses. In March 2010, the Massachusetts Office of Consumer Affairs and Business Regulation
implemented data security regulations\footnote{201 M. MASS. CODE REGS. §§ 17.01-.05 (implementing MASS. GEN. LAWS ANN. Ch. 93H).} to implement the Massachusetts Data Breach Notification Law. The
regulations require every entity that owns or licenses personal information of Massachusetts’s residents\footnote{§ 17.03(1).}
to create a “comprehensive information security program . . . contain[ing] administrative, technical, and physical
safeguards.”\footnote{§ 17.03(1).} Compliance requires identifying reasonably foreseeable security threats, imposing disciplinary
measures for internal violations, and overseeing third-party service providers by requiring the third parties to
maintain appropriate security measures.\footnote{§ 17.03(2).} These data security regulations also set out specific requirements for
computer system security of web operators storing data about Massachusetts residents, including the (1) use of
secure authentication protocols, (2) use of unique IDs and passwords for each system user, (3) encryption of all
personal data transferred on public networks, (4) periodic system monitoring, (5) fire wall use, and (6) the use of the
most current versions of system security software.\footnote{§ 17.04(1)-(3).} Knowingly failing to provide the required notice or violating
the data security regulations can result in a civil penalty of up to $5,000 for each compromised data record,\footnote{Mass. Gen. Laws Ann. Ch. 93H, § 4.} which
can accumulate quickly for a large breach. The state attorney general and individuals can sue for damages and an
injunction.\footnote{§ 4.}
A class action lawsuit against Google, Inc. might be the first case to allege a violation of the data security regulations of the Massachusetts Data Breach Notification Law. In *Galaxy Internet Service, Inc. v. Google, Inc.*, the plaintiff was a WiFi network operator in Boston, and the network carried personal data of Massachusetts residents. The WiFi operator alleged that Google’s Street View vehicles violated the regulations when they secretly captured data transferred on the WiFi network, decoded or decrypted it, and stored it on servers accessible by hundreds of people. The case is still pending.

### State Common Law

Internet users may look to the tort of “intrusion upon seclusion” for remedies against invasions of privacy arising out of e-mail and Internet usage. To make a cognizable claim, the Internet user must show that the alleged intrusion would be highly offensive to a reasonable person. Generally, employees have been unsuccessful in asserting this theory to prevent workplace e-mail monitoring.

### FTC ENFORCEMENT AND INITIATIVES

#### Organization and Authority

Starting with its 2001 twelve-point privacy agenda, the FTC has encouraged consumers to register privacy complaints with it. In 2006, the FTC created the Division of Privacy and Identity Protection within its Bureau of Consumer Affairs. In addition to enforcement of privacy-related statutes and regulations, this division joined with the Department of Justice and state attorneys general to attack the problem of identity theft, and it operates the Identity Theft Data Clearinghouse, the national repository for tracking identity theft complaints.

The FTC has authority over privacy issues in several ways. First, COPPA, the GLB Act, and the FCRA explicitly grant enforcement power to the FTC. The FTC implements those statutes by adopting and enforcing rules. The FTC also cooperates with HHS in connection with security breach notification requirements imposed upon providers of electronic health records. Additionally, the FTC regulates unfair and deceptive acts and practices affecting interstate commerce pursuant to Section 5 of the FTC Act. The FTC uses this authority to regulate

---

436 Id. at 2-3, 5-6, Galaxy Internet Services, Inc. v. Google, Inc., No. 5:2010cv03640 (N.D. Cal. Aug. 24, 2010).
437 Id. at 4-5.
439 See Restatement (Second) of Torts § 652B (1977).
444 See supra notes 250-287 and accompanying text.
445 See supra notes 144-184 and accompanying text.
446 See supra notes 185-198 and accompanying text.
online privacy practices. Specifically, the FTC has been heavily involved in consumer protection related to advertising, which frequently involves online activity. Outside the narrow confines of regulations of financial, health, and children’s information, the FTC does not have specific, delineated, statutory authority to regulate privacy. The agency has sought rulemaking authority and used its authority under Section 5 to take a leading role in efforts to regulate the collection, use, and disclosure of information online. Three bills pending in Congress in 2012 propose comprehensive federal privacy regulation with enforcement falling to the FTC. The FTC’s leading role in this area is expected to continue.

**FTC Enforcement Actions**

The FTC has explicitly pursued an “aggressive, pro-consumer, privacy agenda,” which has resulted in the settlement of many privacy and data security-related investigations. These settlements often include large fines. For example, the FTC obtained settlements with Eli Lilly, Jolly Time Popcorn, Etch-a-Sketch, Hershey Foods Corporation, Mrs. Fields Cookies, Twitter, Sony BMG, Sears, Facebook, Google, MySpace, and others. Many recent settlements alleged failures to take reasonable security measures to safeguard confidential consumer information or to adequately disclose the extent of sensitive personal information collected from consumers. The following examples describe these enforcement actions in more detail.

The action against Toysmart.com is an important example of early FTC enforcement. Toysmart.com was an online toy retailer that collected detailed personal data about its users, including billing information and shopping preferences. It also collected personal profile data, including the names and birth dates of children. Toysmart.com fell within COPPA oversight, because it was directed to children and collected children’s data with actual knowledge. Toysmart.com posted a privacy policy stating that it would never sell the collected personal data to third parties. When the company foundered, however, it filed for bankruptcy. It sought to sell its assets, including its database of personal data. The FTC sued to enjoin the sale of the database, citing the FTC’s authority to prevent unfair or deceptive acts or practices under Section 5 of the FTC Act. To settle the action,
Toysmart.com agreed to sell its database only to a qualified buyer. A qualified buyer was one that agreed to uphold the terms of the original Toysmart.com privacy policy and would not deviate from the allowed uses under that privacy policy without permission from the affected customers. Several state attorneys general criticized the settlement and objected to a proposed sale of the database in the bankruptcy court. The bankruptcy court did not approve the sale. Finally, the Walt Disney Company (a corporate affiliate of Toysmart.com) purchased the database for $50,000 and destroyed it. Toysmart.com remains a landmark case for both privacy advocates emboldened by the outcome and corporations chastened by it.

A similar case recently occurred upon bankruptcy of Borders Group Inc. It owned a database containing customer information and wanted to sell it during bankruptcy proceedings. The FTC expressed to the court its concern about the transfer of personal information. In September 2011, the bankruptcy court agreed to the sale of the database to former competitor Barnes & Noble Inc. and ordered that all former Borders’ customers be notified by e-mail that they can choose not to have their personally identifiable information transferred with the sale. If a customer chooses not to opt out of the transfer, virtually all data, regardless of whether he previously opted not to share it, will be transferred to Barnes & Noble.

The FTC has initiated enforcement actions for failure to secure personally identifiable information. For example, in 2009, the FTC investigated how the pharmacy chain CVS Caremark (“CVS”) disposed of pill bottles and other items containing sensitive information. According to complaints filed with the FTC, CVS discarded “materials containing personal information in clear readable text (such as prescriptions, prescription bottles, pharmacy labels, computer printouts, prescription purchase refunds, credit card receipts, and employee records) in unsecured, publicly-accessible trash dumpsters on numerous occasions.” The FTC alleged that CVS failed to appropriately safeguard and dispose of its customers’ and employees’ sensitive financial and health information, despite CVS’s stated policy to maintain its privacy. In the settlement with the FTC, CVS agreed to implement a comprehensive information security program. The FTC and the Department of Health and Human Services (“HHS”) jointly challenged CVS’s data security of its employee data under HIPAA in a separate action. CVS agreed to establish another comprehensive information security program as well as pay $2.25 million to the HHS.

The FTC also investigates claims that an organization failed to inform customers about what information it collected and how that information was used. As an example, the FTC brought an action against Sears Holding Corporation. In 2008, Sears was facing bankruptcy proceedings. It was selling single-use pill bottles to customers, and the FTC alleged that this practice enabled customers to reuse bottles to contain personal information. The FTC alleged that CVS failed to appropriately safeguard and dispose of its customers’ and employees’ sensitive financial and health information, despite CVS’s stated policy to maintain its privacy. In the settlement with the FTC, CVS agreed to implement a comprehensive information security program.

The FTC and the Department of Health and Human Services (“HHS”) jointly challenged CVS’s data security of its employee data under HIPAA in a separate action. CVS agreed to establish another comprehensive information security program as well as pay $2.25 million to the HHS.

---

467 Id.
468 Id.
469 Id.
472 Id. ¶¶ 6-7.
473 CVS Decision, supra note 454, at 3-4.
Management Corporation ("Sears"). Consumers of Sears could participate in market research by downloading software from sears.com and kmart.com.\textsuperscript{475} Sears represented to consumers that the software would confidentially track their online browsing.\textsuperscript{476} A long user agreement accurately described the data being monitored, but the description was not included in the marketing materials. The FTC alleged that Sears failed to adequately disclose that the software monitored consumers’ online secure sessions and tracked some computer activities unrelated to the Internet, which were unfair and deceptive trade practices under Section 5 of the FTC Act.\textsuperscript{477} In the settlement, Sears agreed to clearly, prominently, and separately from the user license agreement, disclose the types of data monitored, recorded, or transmitted prior to software installation.\textsuperscript{478} Sears also agreed to destroy the information previously collected.\textsuperscript{479} This settlement illustrates what the FTC deems adequate notice of data collection practices to consumers and sufficient consent when privacy concerns may be present. It also indicates that the FTC is willing to find a deceptive practice where marketing or related information is inconsistent with disclosures found only in a privacy statement or similar document.

In 2005, the FTC investigated two notable information security breaches at retail stores. In the first action, the FTC alleged that BJ’s Wholesale Club (“BJ’s”) failed to secure the sensitive information of thousands of its customers, which was an unfair business practice under Section 5 of the FTC Act.\textsuperscript{480} According to the complaint, BJ’s did not encrypt customer data stored in its network, stored customer data in files that could be accessed anonymously, failed to employ available security measures, and created an unnecessary risk by storing customer data for up to thirty days. BJ’s alleged that a rash of fraudulent purchases using counterfeit copies of credit cards with numbers matching those used at BJ’s resulted from these lax data security practices.\textsuperscript{482} BJ’s faced direct liability to their customers, and in the resulting FTC settlement it agreed to implement a costly information security program and undergo biannual, independent audits of its information security for the next twenty years.\textsuperscript{483} Notably BJ’s did not have an information security policy and made no claims as to the security of the personal data it stored.\textsuperscript{484} For that reason, this action was a drastic departure from previous FTC actions which required an explicit promise to be broken and is considered significant because of the FTC’s use of its “unfairness” authority to regulate data security.

Soon after the BJ’s settlement, the FTC instituted a similar action against shoe retailer DSW for failing to protect sensitive data.\textsuperscript{485} DSW’s lax data security methods compromised the security of an estimated 1.4 million credit and debit cards and 95,000 checking accounts.\textsuperscript{486} The settlement terms with DSW were similar to the BJ’s settlement.\textsuperscript{487} After a series of high-profile security breaches with the intentional disclosure of consumer credit reports to unauthorized entities, the FTC investigated violations of the FCRA and the FTC Act against ChoicePoint in 2006.\textsuperscript{488}

\textsuperscript{476} Id. ¶ 6.
\textsuperscript{477} Id. ¶ 13.
\textsuperscript{478} Id.
\textsuperscript{479} Sears Decision, supra note 454, at 5.
\textsuperscript{482} Id. ¶¶ 8-9.
\textsuperscript{483} BJ’s Press Release, supra note 480.
\textsuperscript{484} See also Twitter, Inc.; Analysis of Proposed Consent Order to Aid Public Comment, 75 Fed. Reg. 37806 (June 30, 2010); Twitter, Inc., 2010 ILRWeb (P&F) 2081, FTC Docket No. C-4316, at 2 (June 24, 2010).
\textsuperscript{486} Id.
The settlement resulted in the largest payout in FTC history—$10 million in fines and $5 million in restitution to approximately 14,000 customers who had out of pocket costs as a result of a data breach. ChoicePoint collected personal data and sold the aggregated data to businesses as credit reports. Unlike most of the FTC enforcement cases previously discussed, the weak link in ChoicePoint's security was its policy and not its technology. The FTC alleged that ChoicePoint violated the FCRA when it knowingly distributed over 163,000 consumer reports to entities unauthorized to obtain or use consumer reports resulting in over 800 cases of identity theft. ChoicePoint also allegedly ignored red flags designed to indicate unauthorized requests. In addition, ChoicePoint publicly communicated that it provided consumer information only to authorized parties under the FCRA, but in fact it distributed the information to many unauthorized parties. The FTC considered this action a misleading practice under Section 5 of the FTC Act.

In 2010, the FTC sued Twitter for failing to properly safeguard consumers’ personal information. Hackers twice gained administrative access to Twitter by guessing a “weak” password and by hacking an employee’s email account to find a password. Hackers sent out fake tweets from real accounts, accessed non-public user information, and saw private tweets. In its privacy policy and other statements on its website, Twitter stated that it employed “administrative, physical, and electronic measures” to protect user data from unauthorized access. The FTC alleged Twitter “deceived consumers and put their privacy at risk by failing to safeguard their personal information,” because it engaged in several practices that did not take sufficient precautions to ensure administrative access was difficult to hack. Because the FTC concluded that Twitter had stated it took reasonable security measures, but failed to do so, the FTC alleged that Twitter made false or misleading misrepresentations resulting in a violation of Section 5 of the FTC Act. The FTC required that Twitter could not misrepresent its security measures and must implement a comprehensive data security program, which must be independently audited biannually for ten years.

The FTC recently took aim at some of the biggest names on the Internet. As a result, Google, Facebook, and MySpace all agreed to consent orders. Google’s release of Google Buzz made headlines for its automatic sharing of user data. In 2010, Google attempted to enter the social networking industry with its Buzz product. Without user consent, converted all of its Gmail product users into Buzz users. When Buzz was launched, Gmail users were shown a screen announcing Buzz and asking users if they wanted to use it. Regardless of how users

---

489 Id.
491 Id. ¶¶ 12, 15-22 (citing 15 U.S.C. §§ 1681b(a), 1681e(a)).
492 Id. ¶¶ 15-22 (citing 15 U.S.C. §§ 1681b(a), 1681e(a)).
493 Id. ¶¶ 27-36.
494 Id. ¶ 1.
496 Id. at 167-68.
497 Id. at 165.
498 Id. at 166-67. The practices include failing to (1) establish and enforce policies to make password hacking difficult, (2) prohibit storage of administrative passwords in personal e-mail accounts, (3) disable passwords after a reasonable number of failed log-in attempts, (4) separate administrative log-ins from the normal Twitter log-in process, (5) enforce periodic administrative password changes, (6) restricting administrative access to only necessary employees, and (7) imposing administrative access to specified IP addresses.
499 Id. at 168-69.
500 Id. at 172-175.
503 Id. ¶ 7.
504 Id. ¶ 8.
responded, Gmail users’ public profile information was shared in Buzz until the users proactively opted out. In the Gmail privacy statement, Google promised to obtain Gmail users’ permission before using their data for anything other than providing the Gmail service. The FTC alleged that “the setup process for Gmail users who enrolled in Buzz did not adequately communicate that certain previously private information would be shared publicly by default.” The FTC also alleged that the Buzz privacy control tools were confusing and difficult to use. Google agreed to obtain express affirmative user consent before sharing data differently than when the data was originally collected and implement a comprehensive data security program, which must be independently audited bimannually for twenty years. Class action lawsuits for the same action resulted in Google agreeing to pay an $8.5 million award split among fourteen privacy organizations and nonprofits.

Facebook allegedly made false representations to consumers regarding its privacy practices, such as when Facebook shared information with third parties. In particular, the FTC was concerned about Facebook’s alleged data sharing with third-party applications and advertisers different from the sharing practices described in its privacy policy. In resolving the complaint, Facebook agreed not to make misrepresentations about its privacy practices, and that it must provide notice and obtain affirmative express consent from users when it shared “nonpublic user information” in ways that exceeded users’ privacy settings. Moreover, Facebook is required to establish and maintain a comprehensive privacy plan, audited independently for the next 20 years.

Similar to Facebook, the FTC alleged that MySpace misled users about sharing personal information with third-party advertisers. As a result, MySpace may not make future misrepresentations about its privacy policies. Further, like Google and Facebook, MySpace is required to establish and maintain a comprehensive privacy plan, audited independently for the next 20 years.

**FTC Guidance**

The great increase in privacy-related enforcement initiatives coincides with increased FTC guidance. For example, the FTC released a guide entitled Protecting Personal Information: A Guide for Business (the “FTC Business Guide”) which provides detailed instructions on reasonable and appropriate steps businesses should take to protect their customers’ and employees’ personal information. The FTC Business Guide provides accessible best practice counseling for how all business should handle personal information. Up to this point, federal and state statutes related to privacy and data security pertain to a particular class of data or single industry. Usually, there is no guidance on implementing such class-specific security measures. Therefore, the FTC guides provide welcome help to businesses attempting to navigate the patchwork of complicated privacy and data security law.

**A. The Business Guide**

---

[^505]: Id.
[^506]: Id. ¶ 6.
[^507]: Id. ¶ 9.
[^508]: Id.
[^513]: Id.
[^516]: Id.
The FTC Business Guide serves as a helpful baseline to help companies manage information security risks. It provides five principles that businesses should follow when implementing a security plan. These principles are as follows:

- **Take Stock.** Know what personal information you have in your files and on your computers.
- **Scale Down.** Keep only what you need for business.
- **Lock It.** Protect the information you keep.
- **Pitch It.** Properly dispose of what you no longer need.
- **Plan Ahead.** Create a plan to respond to security incidents.  

### B. Information Practices Guidance

As set forth succinctly in the FTC guidelines, every consumer-oriented website should provide:

- **Notice.** Websites should provide consumers clear and conspicuous notice of their information practices, including what information they collect, how they collect it, e.g., directly or through non-obvious means such as cookies, how they use it, how they provide Choice, Access, and Security to consumers, whether they disclose the information to third parties, and whether other entities are collecting information through the site;
- **Choice.** Websites should offer consumers choices as to how their personally identifying information is used beyond the use for which the information was provided, e.g., to perform a transaction. Such choice should encompass both internal secondary uses (such as marketing back to consumers) and external secondary uses (such as disclosing data to third parties);
- **Access.** Websites should offer consumers reasonable access to review the information a website has collected about them and to correct inaccuracies or delete it; and
- **Security.** Websites should take reasonable steps to protect the security of the information they collect from consumers.

Many websites’ privacy policies now reflect these guidelines, because they fear federal legislation if they do not alleviate consumers’ concerns about online privacy protection.

### C. Online Behavioral Advertising Guidance

In addition to best practices counseling, the FTC has also provided guidance for self-regulation of online behavioral advertising (“OBA”). OBA, as defined by the FTC, is the collection of information about a person’s online activities over time to serve advertisements tailored to that person’s interests. Information used for behavioral advertising typically does not identify a person by name, address, or other similar identifier, and therefore is not “personally identifiable” in the traditional sense. Rather, information is collected and associated with a particular computer or other device, often through the use of cookies and similar technologies. The practice raises privacy concerns nonetheless, because users are generally unaware this data collection occurs, and the information about their preferences and interests—some of which may be significant in nature or amount—could potentially be misused or compromised.

---

518 Id.
520 Id. at iii.
522 Id. at 2.
523 Id.
524 Id.
525 Id. at 6-10.
To address the privacy concerns, the FTC proposed principles for self-regulation in 2007. The guidance outlined issues and principles for each of the following goals: (1) transparency and consumer control; (2) reasonable security and limited data retention of consumer data; (3) affirmative express consent for material changes to existing privacy promises; and (4) affirmative express consent to (or prohibition against) using sensitive data for behavioral advertising. Further, the agency requested input regarding a fifth area, the use of tracking data for purposes other than behavioral advertising. Following public comment on the proposed goals and principles, in 2009, the FTC clarified the principles apply to any data that “reasonably could be associated with a particular consumer or computer or other device.” These principles, however, do not apply to “first party” behavioral advertising (collection of information on a website for advertisement delivery on that same website) or “contextual” advertising (advertisement targeting based on a website being viewed or a search query).

The 2009 Report reiterated and expanded the four principles outlined in 2007. First, the FTC restated that website operators should provide clear and prominent notice of behavioral advertising separate from their privacy policies and supply accessible methods for consumers to opt out. Second, web operators should minimize retention and provide “reasonable security” for data collected for behavioral advertising purposes. The security measures should be tailored to consider the sensitivity of the data and risks associated with each particular web operator. Third, the FTC clarified that a chief concern is material, retroactive changes to a privacy policy, because they affect data a company collected prior to the changes. Web operators should obtain affirmative, express consent before using behavioral data in a manner that differs materially from promises made when the company collected the data. Fourth, the FTC encouraged web operators to obtain express consent before collecting “sensitive data” for behavioral advertising purposes.

In light of the FTC’s focus on OBA and general public concern about the practice, a coalition of advertising organizations, the Digital Advertising Alliance (the “DAA”), developed a self-regulatory regime featuring the Advertising Option Icon. The icon is part of the industry’s implementation of its “Self-Regulatory Principles for Online Behavioral Advertising,” (“the Principles”) released in 2009. The DAA principles are based on the principles listed in the FTC’s 2009 staff report: consumer education, transparency of OBA practices, consumer control of OBA practices, security of OBA data, consent prior to material changes to OBA

526 See id.
527 Id. at 11-12.
528 Id. at 12.
529 Id. at 25.
530 Id. at 26-30. The report notes, however, that regardless of the scope of these principles, companies still must comply with all applicable privacy laws, some of which may impose requirements that are similar to those established by the principles. Id.
531 Id. at 35-36.
532 Id. at 38.
533 Id.
534 Id. at 40-41.
535 Id. at 43-44.
537 OBA PRINCIPLES, supra note 536.
538 Id. at 1 (giting Fed. Trade Comm’N, Self-Regulatory Principles for Online Behavioral Advertising (2009)).
539 Id. at 28-29.
540 Id. at 12-14. The DAA requires both principle websites and third-party advertisers to provide notice to consumers regarding the types of data collected in OBA and the use of such data. Id. Third-party advertiser should indicate that data is being collected either near the advertisement or on the page on which the data is collected. Id. Principle websites should indicate the use of third-party advertisers on the page where data is collected. Id.
541 Id. at 33-35. Participants should provide users with a way to control the collection and use of data via the participant’s website or an industry-developed website. Id.
practices,\textsuperscript{543} avoiding OBA collection of sensitive data,\textsuperscript{544} and accountability through self-monitoring.\textsuperscript{545} With its Principles, the DAA sought to develop a “robust and credible” self-regulatory regime, which included a complaint procedure and the opportunity for Internet users to opt out.\textsuperscript{546}

The Advertising Option Icon appears in the corner of a behaviorally targeted advertisement, and clicking on it will explain how to opt-out.\textsuperscript{547} The icon is licensed by DAA, a collection of associations including the Council of Better Business Bureaus (“CBBB”).\textsuperscript{548} By using the clickable icon, advertisers can provide consumers in-ad notice and choice that is easy to access and understand.\textsuperscript{549} The CBBB monitors compliance, and those that fail to correct non-compliance face public disclosure, referral to regulatory authorities, and exclusion from trade associations.\textsuperscript{550} As of December 2012, the DAA has over 400 participating companies.\textsuperscript{551} “So long as self-regulation is making forward progress,” said FTC Chairman Jon Leibowitz in reaction to the DAA’s self-regulatory principles, “the FTC is not interested in regulating in this area.”\textsuperscript{552}

Despite FTC guidance, threatened enforcement, and industry self-regulation, online behavioral advertisers continue to be investigated. In 2011, the FTC investigated a company performing OBA. Chitika, Inc. is an OBA company that contracts with websites to provide targeted advertising to users.\textsuperscript{553} To customize advertising for website users, Chitika tracks their Internet surfing with cookies.\textsuperscript{554} Chitika’s cookies lasted indefinitely, but users were allowed to opt out of tracking.\textsuperscript{555} Chitika failed to disclose the opt-out period only lasted ten days, after which the tracking restarted when a user visited a website using Chitika’s services.\textsuperscript{556} The FTC alleged that Chitika violated Section 5 of the FTC Act when it represented, by implication, that opting out would last for a reasonable period of time, and ten days was not a reasonable period of time.\textsuperscript{557} In the consent order, Chitika agreed its opt-out period would thereafter last for at least five years.\textsuperscript{558}

D. The FTC’s 2012 Report on Privacy

\textsuperscript{542} Id. at 15-16. Participants should employ “physical, electronic, and administrative safeguards” to protect user data and should retain data for only as long as necessary “to fulfill a legitimate business need.” Id. at 15. Also, the DAA calls on participants to “alter, anonymize, or randomize” personally identifiable information as well as to take reasonable steps to protect anonymized data if distributed to third parties. Id. at 15-16.

\textsuperscript{543} Id. at 16. “Material changes” do not include changes that result in the collection of less data. Id.

\textsuperscript{544} Id. at 16-17. Participants should not collect the personal information of children. Id. Nor should participants collect, without consent, financial account numbers, Social Security numbers, or medical records or prescriptions. Id.

\textsuperscript{545} Id. at 17-18, 41-42. Accountability programs consist of systematic compliance monitoring, reporting non-compliance, and subsequent steps to bring the program into compliance. Id. at 17-18.


\textsuperscript{547} OBA PRINCIPLES, supra note 536, at 5; Hearing on “Understanding Consumer Attitudes About Privacy Before the Subcomm. On Commerce, Manufacturing and Trade of H. Comm. on Energy and Commerce,” 112th Cong. 9 (2011) (statement of Linda Woolley, Member, Board of Directors, Digital Advertising Alliance) [hereinafter DAA Testimony].

\textsuperscript{548} DAA Testimony, supra note 547, at 10-11.

\textsuperscript{549} OBA PRINCIPLES IMPLEMENTATION, supra note 536, at 2.

\textsuperscript{550} Id. at 2-3; DAA Testimony, supra note 547, at 12.

\textsuperscript{551} Peter Kosmala, DAA Celebrates its First Anniversary (Oct. 25, 2011 4:45 PM), http://www.aboutads.info/blog/daa-celebrates-its-first-anniversary. The DAA indicates that participant companies “include all 15 of the Top 15 online advertising networks among them Google, Yahoo! and AOL.” Id.


\textsuperscript{554} Id. at 495.

\textsuperscript{555} Id. at 496-97. Chitika stored information about a given user for up to two years. Id.

\textsuperscript{556} Id. at 497.

\textsuperscript{557} Id. at 498 (citing 15 U.S.C. § 45(a)).

\textsuperscript{558} Id. at 505.
Two years after FTC staff issued a proposed privacy framework, the FTC released its final Privacy Report in early 2012, *Protecting Consumer Privacy in an Era of Change: Recommendations for Businesses and Policymakers* (“FTC Privacy Report”). The FTC Privacy Report is not the law, but it provides the FTC’s view on best practices regarding the collection, use, and disclosure of consumer data. The report proposed a framework for addressing privacy issues based upon three general principles: privacy by design, simplified choice, and greater transparency. The FTC’s privacy framework applies broadly to “all commercial entities that collect or use consumer data that can be reasonably linked to a specific consumer, computer, or other device” when the entity collects data from more than 5,000 consumers a year or shares the data with third parties. This includes consumer information collected or used both online and offline. The FTC no longer focuses solely on entities that collect personally identifiable information, as the FTC determined that this classification has become increasingly meaningless.

**Privacy by Design.** The FTC proposed the baseline principle: “Companies should promote consumer privacy throughout their organizations and at every stage of the development of their products and services.” Among the substantive protections the FTC would like to see are: reasonable security for consumer data, reasonable collection limits, sound retention practices, and measures to ensure data accuracy.

Under the framework, companies should limit data collection to what is consistent with the context of the transaction or the relationship between the company and consumer, or what is required or specifically authorized by law. In other words, the FTC wants companies to consider whether their data collection is consistent with what a consumer reasonably would expect based on the context of the transaction or business relationship. Where the collection would not be consistent with consumer expectations at the time of collection, the framework encourages companies to provide prominent notice and choice to the consumer outside of a privacy policy or other legal document.

The principle includes limiting the retention of data and disposing of it once it has outlived the purpose for which it was collected. Moreover, the framework adopts a flexible approach asking companies to take reasonable steps to ensure the accuracy of the data collected and maintained, depending on where the data could be used to cause significant harm or to deny services to consumers.

The FTC also recommends that businesses should implement “comprehensive data-management procedures throughout their product or service lifecycles.” These procedures may include designating privacy personnel responsible for training employees regarding privacy practices, conducting regular privacy assessments, and developing privacy-enhancing technologies, such as encryption and anonymization tools.

**Simplified Choice.** The FTC sought to simplify consumer choices regarding their online privacy. The FTC Privacy Report focuses on the context of the interaction between the consumer and the business. Under this principle, companies do not need to provide choice before collecting and using consumers' data for practices that are consistent with the context of the transaction or the company's relationship with the consumer, or when the

---

560 *Id.* at iii.
561 *Id.* at vii, viii (2012).
562 *Id.* at iv.
563 *Id.* at 17.
564 *Id.* at 22.
565 *Id.* at 23.
566 *Id.* at 27.
567 *Id.*
568 *Id.*
569 *Id.* at 28.
570 *Id.* at 30.
571 *Id.* at 32.
572 *Id.* at 30-31.
573 *Id.* at 38.
collection or use is required or expressly authorized by law.\textsuperscript{574} The report notes that five “commonly accepted” practices (i.e., order fulfillment, internal operations, fraud prevention, legal compliance, and most first-party marketing) generally will meet this standard.\textsuperscript{575} The FTC specifically identified the sale of consumer information to a third party and the tracking of consumers across third-party websites as practices that \textit{would} require notice and choice under the framework.\textsuperscript{576} Even the sharing of consumer data among affiliated companies should be disclosed, unless the affiliate relationship is clear to consumers.\textsuperscript{577}

The report endorses obtaining affirmative, express consent from consumers before collecting sensitive data, such as information about children, finances, or health, regardless of the use of such data.\textsuperscript{578} Similarly, the report states that companies should obtain affirmative, express consent before making material, retroactive changes to privacy representations.\textsuperscript{579}

The FTC Privacy Report continues to advocate for the implementation of a "Do Not Track" mechanism that would give consumers choice with respect to online behavioral tracking.\textsuperscript{580} The report sets forth five key principles to make such a system effective, it must: (1) be implemented universally to cover all parties that would track consumers; (2) be easy to find, easy to understand, and easy to use; (3) have choices that are persistent; (4) be comprehensive, effective, and enforceable; and (5) opt consumers out of the \textit{collection} of behavioral data for all purposes other than those that would be consistent with the context of the interaction.\textsuperscript{581}

\textit{Greater Transparency.} This principle states that companies should make privacy policies clearer, shorter, and more uniform so that consumers, regulators, and others more easily may compare policies among different companies.\textsuperscript{582} The FTC believes that uniformity of privacy notices can be achieved by industry sector.\textsuperscript{583} In addition, the FTC Privacy Report endorses a sliding-scale approach to providing consumers with reasonable access to data about them.\textsuperscript{584} Companies should adjust consumers' ability to access data about them based on the use and sensitivity of the data.\textsuperscript{585} The report asserts that, at minimum, companies should offer consumers access to (1) the types of information companies maintain about them and (2) the sources of such information.\textsuperscript{586} The Commission endorsed the practice of companies providing consumers with access to a list of categories of data they hold, and the ability to opt out of its use for marketing.\textsuperscript{587}

The FTC continues to focus on online privacy issues as new technologies create new privacy challenges. In the report, the FTC identified five areas of future focus: (1) developing an effective do-not-track system, (2) improving disclosures to mobile consumers, (3) supporting regulation of data brokers, (4) tracking by large online platform providers, and (5) facilitating sector-specific codes of conduct.\textsuperscript{588} Businesses are well-advised to stay abreast of FTC regulations and guidance, especially when the media draws attention to the privacy impact of a given technology.

E. Mobile

\textsuperscript{574} Id. at 38-39.  
\textsuperscript{575} Id. at 39.  
\textsuperscript{576} Id. at 39, 41.  
\textsuperscript{577} Id. at 41-42.  
\textsuperscript{578} Id. at 47.  
\textsuperscript{579} Id. at 58.  
\textsuperscript{580} Id. at 52-55.  
\textsuperscript{581} Id.  
\textsuperscript{582} Id. at 64.  
\textsuperscript{583} Id. at 62.  
\textsuperscript{584} Id. at 67.  
\textsuperscript{585} Id.  
\textsuperscript{586} Id.  
\textsuperscript{587} Id. at 65.  
\textsuperscript{588} Id. at 72-73.
As the FTC promised in its Final Privacy Report, it has increased its focus on the privacy implications of mobile applications. In August 2012, the FTC released its Guide on Marketing Your Mobile App \(^{589}\) where it applied many of the same principles it outlined in its Final Privacy Report. Like its other guidance, the FTC recommended that app developers:

- engage in Privacy by Design;
- add transparency to their privacy practices by clearly disclosing how they collect, use, and disclose information collected from users;
- provide users with privacy controls;
- obtain consent from users before collecting sensitive data such as medical, financial and location information;
- take reasonable steps to secure data;
- ensure it complies with COPPA; and
- honor privacy promises.

While the guide is not the law, the FTC may expect mobile applications to follow these principles as it more closely watches their privacy practices.

**EUROPEAN UNION AND OTHER NON-U.S. INITIATIVES**

**The EU Directive**

**A. Privacy and Data Protection**

The European Union’s Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (the “Directive”), \(^{590}\) was the first large-scale attempt to enforce “privacy of the data subject” and treats individual privacy as a fundamental human right. \(^{591}\) Under the Directive, data privacy encompasses the rights to maintain the confidentiality, integrity, and accuracy of personal information. \(^{592}\) It stated that the principles related to data quality require personal data to be: (1) processed fairly and lawfully; (2) collected for specified, explicit, and legitimate purposes and not further processed in a manner that is inconsistent with those purposes; (3) adequate, relevant, and not excessive in relation to those purposes; (4) accurate and kept up to date; and (5) not kept in a form that permits identification of data subjects for longer than necessary for the purposes for which it was collected or further processed. \(^{593}\)

The Directive requires European Union (“EU”) Member States to enact national legislation that grants individuals basic rights with regard to the processing of their personal data. \(^{594}\) The Member States enact similar, but not identical, laws. Each Member State enforces its national version of the Directive through administrative and criminal proceedings. The national laws require businesses that process data in Europe to register with the Member State where the physical processing occurs.

The Directive also requires EU Member States to enact legislation prohibiting the transfer of personal data to countries outside the EU if those non-member countries do not to ensure an “adequate level of protection.” \(^{595}\) The Directive’s prohibition on data transfers to countries with lower levels of privacy protection could prevent transfers of personal data from EU Member States to the United States and other countries. Stopping data transfers could have significant consequences for virtually every sector of the economy, especially the direct marketing industry and...

---


\(^{591}\) Id. at art 13(2).

\(^{592}\) See id. at art. 6(1).

\(^{593}\) Id.

\(^{594}\) Id. at arts. 31-32.

\(^{595}\) Id. at art. 25(1).
intra-corporate human resources functions (whether Internet-based or not). EU officials concluded that privacy protections in the United States did not ensure an adequate level of protection. To avoid an embargo on personal data flows from the EU to the United States, the U.S. Department of Commerce (“DOC”) negotiated a stay of enforcement to temporarily allow data transfers to the U.S. To cure the deviation between U.S. standards and EU requirements, the DOC took the dual role of negotiating with the EU while also urging stricter U.S. data protection standards, both legal and industry-sponsored. Those efforts culminated in the EU’s approval of the Safe Harbor Principles in July 2000 and in the implementation of them by the United States.

This section briefly summarizes the Directive’s provisions and enforcement mechanisms. Additionally, this section provides information on how U.S. companies can comply with the Directive to avoid interruptions in the cross-border transfer of personal data.


“Processing” and “Personal Data.” The Directive places restrictions on the processing of an individual’s personal data. “Processing” includes any set of operations that is performed on personal data, whether automatic or not, such as collection, organization, storage, retrieval, alignment or combination, use, or destruction. The term “personal data” includes “any information relating to . . .” an “identifiable natural person.” The Directive does not apply to data processing related to certain areas involving public security, defense, or criminal law. The Directive also does not apply to processing by “a natural person in the course of a purely personal or household activity.”

The Directive permits the processing of personal data only in the following circumstances:

- The person whose personal data are at issue gives unambiguous consent to the processing.
- The processing is necessary for the performance of a contract to which the data subject is a party or to take steps at the request of the data subject prior to entering into a contract.
- The processing is necessary for compliance with a legal obligation to which the data controller (the person or entity that decides the purposes and means of processing the data) is subject.
- The processing is necessary to protect the vital interests of the data subject.
- The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller or in a third party to whom the data are disclosed.
- The processing is necessary for the legitimate interests of the data controller (or a third party to whom the data are disclosed) unless those interests are overridden by the interests for fundamental rights and freedoms of the data subject.

The Directive also provides special protections for “sensitive data,” which include personal data pertaining to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and health or sex life. Sensitive data may be processed only where the

- data subject has given his explicit consent to the processing (except where Member State law provides that the collection of particular types of data may not be authorized by a data subject’s consent);
- processing is necessary to carry out the obligations and specific rights of the data controller in the field of employment law (to the extent authorized by national law);
- processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent;
- processing is carried out by a foundation, association, or other non-profit entity with a political, philosophical, religious, or trade-union aim in the course of its legitimate activities with appropriate

596 Id. at art. 2(b).
597 Id. at art. 2(a).
598 Id. at art. 3(2).
599 Id.
600 Id. at art. 7.
601 Id. at art. 8(1).
guarantees, where the processing relates solely to the entity’s members or to persons in regular contact with it, in connection with the entity’s purposes, and on the condition that the data cannot be disclosed to a third party without the consent of the data subject; or

- processing relates to data that are manifestly made public by the data subject or that are necessary for the establishment, exercise, or defense of legal claims.\(^{62}\)

Member States may create additional exemptions for reasons of important public interest.\(^{63}\) Special limitations also apply to the processing of data regarding criminal offenses and convictions.\(^{64}\)

“Consent.” Consent can be a valid basis for processing personal data, including sensitive data; however, consent must be informed to be valid.\(^{65}\) Therefore, if disclosures are insufficient, the consent will not be adequate. In the case of sensitive data, the data subject must “explicitly” consent to the collection of the sensitive data.\(^{66}\)

Rights of the Data Subject. Data subjects have a specific right of access to their personal data. A data subject has the right to know whether a data controller processes his personal data, and, if so, he has a right to review that personal data.\(^{67}\) If any of the personal data is incorrect, the data subject has the right to ask the data controller to correct or erase the data.\(^{68}\)

Cross-Border Transfers of Personal Data. As of December 2012, the EU had deemed only the laws of Andorra, Argentina, Canada, Faeroe Islands, Guernsey, Israel, Jersey, the Isle of Man, Switzerland, Uruguay “adequate” to protect personal data,\(^{69}\) and it had blessed the U.S. Safe Harbor.

Exceptions. Even if a particular country lacks adequate data protection, however, personal data may be transferred where

- the data subject has unambiguously consented to the transfer;
- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject’s request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of a data subject between the data controller and a third party;
- the transfer is necessary or legally required on important public interest grounds or for the establishment, exercise, or defense of legal claims;
- the transfer is necessary to protect the vital interests of the data subject; or
- the transfer is made from a register which, according to laws or regulations, is intended to provide information to the public and which is open to some public consultation.\(^{610}\)

Many data transfers from the EU to non-EU countries such as the United States do not fall within one of these exceptions. Such transfers may nevertheless proceed where (1) the data recipient is a U.S. entity that participates in the DOC’s “Safe Harbor” program; (2) the contract between the data controller and data recipient contains the EU’s standardized clauses for protection of personal data; or (3) the data recipient’s “code of conduct” is approved by the EU and its fifteen member states. Each of these exceptions is discussed below.

C. Proposed Data Protection Regulation

---

\(^{62}\) Id. at art. 8(2).

\(^{63}\) Id. at art. 8(4).

\(^{64}\) Id. at art. 8(5).

\(^{65}\) Id. at art. 2(h).

\(^{66}\) Id. at art. 8(2)(a).

\(^{67}\) Id. at art. 10.

\(^{68}\) Id. at art. 12(b).


In 2012, the European Commission proposed to reform the Directive with a Regulation.\(^{611}\) The Commission stated that its current framework was sound, but the implementations were fragmented creating legal uncertainty.\(^{612}\) A Regulation is directly applicable to the EU member states, and the Commission sought to require the same level of data protection and uniform applicability throughout the EU.\(^{613}\) This proposed Regulation must go through the legislative process which could dramatically change the provisions, and the Regulation will not take effect for 2 years from when it is enacted.\(^{614}\)

The Regulation would also make some changes to the existing framework. The use of consent to permit data processing will not apply “where there is a significant imbalance between the position of the data subject and the controller.”\(^{615}\) A company with more than 250 employees would be required to designate a “representative” in the EU who will represent the company before the data protection authority.\(^{616}\) The Regulation introduces the “right to be forgotten,” which requires a data controller to erase all of the personal data about the data subject when the purposes for which the data was collected no longer exists, the data subject withdraws consent to the processing, the processing does not comply with the Regulation, or certain other objections by the data subject.\(^{617}\) The Regulation requires notification of affected individuals and the data protection authority in the event of a data breach.\(^{618}\) Administrative fines for certain violations of the Regulation could reach 2% of the company’s world-wide revenue.\(^{619}\)

D. The Safe Harbor

After intensive negotiations between the European Commission and DOC, the EU approved the DOC’s Safe Harbor Principles in 2000.\(^{620}\) In addition, the United States and Switzerland implemented a U.S.-Swiss Safe Harbor Framework agreement in 2008.\(^{621}\) The Swiss Safe Harbor principles overlap significantly with the EU Safe Harbor, and likewise simplify transfer of personal data from Swiss entities to U.S. entities that self-certify to the DOC.

The Safe Harbor requires entities to implement the following Safe Harbor Privacy Principles (“Principles”) to gain protection under the program:\(^{622}\)

- **Notice:** Entities collecting personal data must provide notice to individuals of the purpose for which they collect and use data, a means to contact the entity with inquiries or complaints, information on the types of third parties to which data is disclosed, and a means to limit data use and disclosure.\(^{623}\)

- **Choice:** Entities collecting personal data must enable individuals to opt out of disclosures of data to third parties or uses other than that for which the data was explicitly authorized. Individuals must be given the explicit choice to opt in if sensitive data is to be disclosed to a third party or used for a purpose other than that for which the data was explicitly authorized.\(^{624}\)

---


\(^{612}\) Id. at ¶ 7.

\(^{613}\) Id. at ¶ 8, 11.

\(^{614}\) Id. at ¶ 2.

\(^{615}\) Id. at ¶ 4.

\(^{616}\) Id. at ¶ 1.

\(^{617}\) Id.

\(^{618}\) Id. at Article 31, 32 at ¶ 1.

\(^{619}\) Id. at Article 79 at ¶ 1


\(^{622}\) 520/2000/EC at art. 1(1).

\(^{623}\) Id. at annex I, at 11.

\(^{624}\) Id.
Onward Transfer: Prior to disclosing personal data to a third party, the disclosing organization must apply Notice and Choice principles. To transfer data to a third party, the entity must confirm that the third party complies with the Principles, the Directive, or another adequate privacy regime. As an alternative, the organization can enter into a written contract with the third party requiring the third party to provide at least the same level of privacy protection as is required by the relevant principles.\textsuperscript{625}

Security: Personal data collectors must take reasonable precautions to protect stored or transmitted data from loss, misuse and unauthorized access, disclosure, alteration, and destruction.\textsuperscript{626}

Data Integrity: Collected data must be relevant to the purpose for which it is to be used, and the entity collecting personal data must take reasonable steps to ensure the data are accurate, complete, and current.\textsuperscript{627}

Access: Entities that collect and store personal data must give individuals access to data held about them and enable them to correct, amend, or delete it. Entities do not have to provide this access if the burden of permitting access is disproportionate to the risks to general privacy interests or another person’s privacy would be violated because of this access.\textsuperscript{628}

Enforcement: At a minimum, mechanisms for ensuring compliance with these Principles should include (i) an independent, available, and affordable mechanism for the resolution of complaints and disputes where damages may be awarded if provided for by applicable law or private sector initiatives; (ii) a procedure to ensure that entities have implemented their commitments to the Principles; and (iii) an obligation to remedy problems arising out of a failure to comply with the Principles and consequences for violators.\textsuperscript{629}

Since its inception in July 2000, almost 3,000 organizations have self-certified to the DOC that they adhere to the Safe Harbor framework.\textsuperscript{630} The European Commission concluded that the Safe Harbor is “off to a relatively trouble-free start,” but that many companies participating in the Safe Harbor do not actually comply with its requirements.\textsuperscript{631} For example, the Commission Staff found that “a substantial minority” of Safe Harbor participants posted a website privacy policy that reflected all seven Safe Harbor principles.\textsuperscript{632}

In 2010, the FTC found that Google’s actions with its Buzz product violated the Safe Harbor principles. Google had self certified that it complied with the Safe Harbor principles.\textsuperscript{633} According to the FTC, Google shared user information without consent and in contravention of the privacy policy users agreed to when the data was collected.\textsuperscript{634} The FTC alleged that these actions violated the Safe Harbor Principles of “notice” and “choice.”\textsuperscript{635} Specifically, the FTC alleged that Google violated the “notice” principle by failing to give users notice before using Gmail user data for “a purpose other than for what it was originally collected.”\textsuperscript{636} The FTC alleged that Google violated the “choice” principle by not giving Gmail users a choice as to how their data was used for a purpose other than for what it was originally collected.\textsuperscript{637} As a result, the FTC prohibited Google from misrepresenting the extent

\textsuperscript{625} Id.
\textsuperscript{626} Id. at annex I, at 12.
\textsuperscript{627} Id.
\textsuperscript{628} Id.
\textsuperscript{629} Id.
\textsuperscript{630} See Safe Harbor List, EXPORT.GOV, https://safeharbor.export.gov/list.aspx (last visited Oct. 24, 2011) (containing an interactive list of all entities that have self-certified under the Safe Harbor program).
\textsuperscript{632} Id. at 6.
\textsuperscript{634} Id. at ¶¶ 13-16.
\textsuperscript{635} Id. at ¶¶ 13-19, 25-26.
\textsuperscript{636} Id. at ¶ 25.
\textsuperscript{637} Id. at ¶ 25.
to which it complied with the Safe Harbor Principles. Similarly, in 2012, the FTC concluded that Facebook’s privacy practices violated the Safe Harbor principles.

Not all entities are eligible for Safe Harbor. Only entities that are subject to the jurisdiction of the FTC or the Department of Transportation may participate in the Safe Harbor. Other entities, such as financial institutions regulated by the Department of Treasury and telecommunications companies regulated by the FCC, are not currently eligible for the Safe Harbor. U.S. financial and telecommunications companies continue to transfer personal data between the United States and Europe pending an EU determination on the adequacy of U.S. laws in these areas. U.S. government officials and industry representatives argue that the FCRA and the GLB Act combine to create “adequate” protection for personal financial data. The EU Commission remains skeptical, however, and its representatives continue to negotiate with the Treasury Department toward a mutually acceptable resolution.

E. Model Contract Clauses

The European Commission also has approved standard contract clauses to be used for transfers of personal data from a data controller in the EU (data exporter) to a controller in a non-EU country (data importer) and from a data controller in the EU to a data processor (often the controller’s subcontractor) located in a non-EU country.

Like the Safe Harbor, the standard contractual clauses are not obligatory for data transfers outside the EU but represent another alternative that companies can select. EU Member States are obligated to recognize that companies or organizations using the standard contract clauses provide adequate protection of personal data.

The standard import/export contract clauses contain legally enforceable declarations that bind parties to two notable promises. First, both the data exporter and the data importer promise to process personal data in accordance with basic data protection rules. Second, both parties agree that individuals may enforce their rights under the contract. Few U.S. companies reportedly have taken advantage of the standard contract clauses approach, because U.S. companies consider these clauses unduly burdensome. National authorities within each of the EU Member States can authorize other ad hoc contractual arrangements for the export of data outside the EU based on national law, as long as the national authorities are satisfied that the particular contracts at issue provide adequate protection.

Standard data processing contract clauses also require the EU exporting entity to instruct subcontractors to treat the data in a manner consistent with the Directive. Like import/export contracts, the data processing requirements do not preclude a Member State from authorizing ad hoc contractual arrangements based on their national laws.

In general, U.S. companies have declined to form data processing model contracts because of, in part, the third-party beneficiary clause. This clause expands liability, and therefore risk, by giving unknown third parties independent enforcement rights.

F. Binding Corporate Rules

Another option for compliance with EU data export limitations is the use of Binding Corporate Rules (“BCRs”). Intended for use by multinational corporations, BCRs are a set of legally binding, internal rules


640 Safe Harbor Workbook § 2, EXPORT.GOV, (last updated May 9, 2011 4:35 PM), http://export.gov/safeharbor/eu/cg_main_018474.asp


643 See 2001/497/EC at 25.

644 See id. (third-party beneficiary clause).

645 Id. at 19.


647 Id. at 5.

governing transfer of personal information within the entity.\textsuperscript{649} For large conglomerates, BCRs allow data, including personal information, to be transferred unhindered across international borders without the need for numerous data security agreements between entities. Initially BCRs appeared to be a promising avenue for EU data export compliance. However, widespread development and implementation of BCRs has not occurred.

To implement BCRs, first, a company must design an internal system of procedures and protocols for information governance that meets EU standards.\textsuperscript{650} Second, a company must have its BCRs approved by the data protection authorities in the EU Member Country from which data is transferred.\textsuperscript{651} Some EU member countries have agreed to a mutual recognition process whereby one “lead” data protection authority is responsible for evaluation and approval, or disapproval, of the BCR application.\textsuperscript{652}

G. Developing a Compliance Program

U.S. entities that receive personal data transfers from the EU should review internal data practices for compliance with the Directive to ensure that the receipt of personal data from the EU continues without disruptions. This internal review may include the following steps:

\begin{itemize}
  \item Evaluate the types of personal data received from EU Member States. Entities may collect personal data regarding employees, customers, and other individuals with whom they do business. Drafting a chart or matrix of the types of personal data collected may be helpful, including an identification of the purposes of collection, retention policies, and any other relevant information. Special attention may be paid to the type and nature of collected information, as the Directive has been increasingly interpreted to include broader classifications of data, such as IP address, as potentially personal data within the meaning of the Directive.
  \item Assess the availability and relative advantages and disadvantages of relying on one or more of the Directive’s exceptions.\textsuperscript{653} The EU may interpret the exceptions narrowly. In addition, assess whether the entity qualifies to enroll in the Safe Harbor and whether the standard contract clauses may suit the entity’s needs.
  \item Select a compliance method and take the necessary steps to implement that method.
\end{itemize}

The EU Privacy Directive and the “Cookie” Rule

In 2009, the EU amended the Directive on Privacy and Electronic Communications (“Privacy Directive”). Among the amendments, the EU enacted the “cookie rule,” which required its Member States to implement regulations forcing website operators to give notice and obtain users’ consent before accessing and storing information on their computers.\textsuperscript{654} Websites use cookies as the primary device to access and store information on a
user’s computer. The rule altered website operators’ previous, more limited, obligation to provide notice and a method to opt out.

The cookie rule does not require users’ consent for all data accessed or stored on their computer by a website. A website may access and store data “strictly necessary” to complete the service it provides to a user. For example, an e-commerce website may access and store data on a user’s computer for the purpose of providing shopping cart functionality, saving passwords, and saving language settings. The cookie rule applies when the website accesses or stores information for a purpose other than the service it provides users. The rule’s heaviest burden will likely settle on the online advertising industry, particularly on behavioral advertising. Companies that perform behavioral advertising rely on cookies to track users’ Internet activity, so they can present users with advertisements matching the users’ interests. Behavioral advertising is likely not “strictly necessary” for most websites.

Implementation of the cookie rule could potentially have disruptive and negative effects on both websites and users, which has led Member States to enact different requirements. Many Member States have abstained from enacting the rule, creating a fluid legal situation. The Privacy Directive suggested that adjusting Internet browser settings might be the appropriate tool for users to express their consent. However, browsers are not yet technologically sophisticated enough to provide the granular level of consent required by the cookie rule. Without this functionality, Member States have had trouble deciding what user consent means from a practical standpoint. The Article 29 Data Protection Working Party published an opinion stating that valid online consent is unambiguous, granular, informed, and verifiable, i.e., requiring opt-in consent for every cookie prior to accessing or storing that cookie.

Member States have found this definition extreme and have not adopted it. Instead, they seem to fall into two camps. More business-friendly Member States have passed laws adopting the browser settings solution and will wait to enforce the cookie rule until Internet browsers have the sufficient functionality. Finland, France, Hungary, Ireland, Luxembourg, Sweden, and the United Kingdom have enacted the cookie rule to allow websites to rely on browser settings. However, regulators in France, Ireland, and the United Kingdom have expressly stated that current browser functionality is insufficient to express consent.

Member States more protective of users’ privacy have implemented a more onerous set of requirements. They generally require a stricter prior opt-in approach where every website must provide notice and consent before cookies can be used. Latvia, Poland, and the proposed legislation in the Netherlands seem to adopt the stricter opt-in requirements. Possible solutions for meeting these requirements include: pop-up consent forms when visiting any web page that accesses or stores a cookie, requiring acceptance to terms and conditions describing the website’s use of cookies before allowing entrance to the website, or allowing users to change website privacy settings.

Member States were expected to comply with the Privacy Directive by May 25, 2011. Only a handful actually met that deadline, and the European Commission commenced legal action against twenty Member States to force compliance. Several Member States subsequently enacted laws; however, many remain noncompliant. Due to
the lack of uniformity and compliance with the cookie rule, the European Commission may begin thinking about directly enforcing it.

This lack of uniformity can have significant consequences for website operators. The Privacy Directive relies on the Directive to resolve conflict of law issues that apply to website operators.662 The Directive applies different rules depending upon whether the website operator is physically based inside or outside the EU. If the website operator is based inside the EU, it must follow the law of the Member State in which it is physically located, i.e., its country of origin.663 If the website operator is based outside the EU, say in the United States, it must follow the law of the Member State where it “makes use of equipment.”664 Privacy protection officials will likely argue that accessing and storing cookies on a computer is making use of equipment in that Member State. Therefore, website operators in the United States should understand and carefully follow the particular cookie rule adopted in each Member State in which they access or store cookies not “strictly necessary” to provide its service. The likely consequence is that website operators will attempt to comply with the strictest cookie rule, so that it complies in every Member State.

The Privacy Directive leaves the determination of appropriate penalties for violations to the Member States.665 For example, the United Kingdom’s regulatory body has the ability to impose a fine up to £500,000 for serious offenses.666 The Privacy Directive states that criminal sanctions may even be appropriate.667

**The EU Privacy Directive and Spam**

The EU’s Privacy Directive668 includes an anti-spam component that generally requires online marketers to obtain consumers’ consent before sending commercial e-mail.669 The Privacy Directive also requires website operators to provide clear information to users about the use and purpose of cookies and spyware, along with information about how cookies may be refused and deleted.670 The Privacy Directive has substantial repercussions for U.S. and European businesses, as it covers all processing of personal data on public electronic communications networks in the EU, including communications sent from the United States or another non-EU country.671

Notwithstanding the ban on unsolicited commercial e-mail, the Privacy Directive allows companies to send commercial e-mail to people with whom the company has an existing relationship.672 For example, an online bookstore can send commercial e-mail to a customer who provided personal contact information to the bookstore during a prior purchase, so long as (1) the merchant gives the customer an opportunity to opt out of marketing communications at the initial purchase; (2) the merchant provides an opt-out opportunity in each e-mail to that customer; and (3) the e-mail concerns products and services similar to those originally purchased by the customer.
The Privacy Directive does not define the scope of similar products or services. Similarly, it does not specify the manner in which companies should obtain consent from customers before sending them commercial e-mail.673

Canada: Personal Information Protection and Electronic Documents Act (“PIPEDA”)

PIPEDA674 roughly parallels the EU Directive and the EU/U.S. Safe Harbor, and it brought Canada into compliance with the EU Directive. PIPEDA requires covered organizations to abide by the “Ten Privacy Principles,” which are

- Accountability;
- Identifying Purposes for which data are collected;
- Consent, generally via opt out;
- Limiting Collection to the minimum reasonably necessary for the Identified Purposes;
- Limiting Use, Disclosure, and Retention;
- Accuracy;
- Safeguards, whether physical or via encryption;
- Openness, meaning making privacy policies known;
- Individual Access, which may be limited under some circumstances and for which a fee may sometimes be charged; and
- Challenging Compliance, meaning a procedure for alleging a breach of the Ten Privacy Principles before the data collection organization and also before Canada’s Privacy Commissioner, complete with a means to sanction the data collection organization and provide money damages to individuals.675

PIPEDA applies mostly to business entities. Exceptions include some government units, individuals who collect or use data only for personal purposes, and entities that collect or use personal data for journalistic, artistic, or literary purposes.676 While some commentators have complained that Canada’s combination of federal and provincial laws is confusing, others note that compliance with the EU Directive necessarily brings concerned businesses into compliance with Canadian laws.

Other International Privacy Laws

In addition to the EU Directive and the enacting legislation, laws of other foreign countries may also affect cross-border data transfers.677 For example, in December 2000, Australia enacted the Privacy Amendment (Private Sector) Act 2000,678 which established a comprehensive data privacy regime applicable to the private sector. Like the Canadian privacy law, the Australian Privacy Act sets out ten “National Privacy Principles” on subjects such as permissible uses and required disclosures, rights of access and correction, and regulation of sensitive information.679 The National Privacy Principles also outline the circumstances under which personal information can be transferred.

---

675 S.C. 2000, c. 5, sched. 1, § 5.
678 Privacy Amendment (Private Sector) Act, 2000, c. 155 (Austl.).
679 2000, c. 155, sched. 3.
outside of Australia. In general, such information can be lawfully transferred only to countries with comparable privacy schemes.

In 2010, the EU completed a comparative study on privacy protections in India and concluded that India’s privacy protections were inadequate. In 2011, India amended its existing Information Technology rules, created under its Information Technology Act. India’s new rules include data privacy protections and ISP privacy requirements. The data privacy rules require consent before entities may collect sensitive information, such as financial, health, and biometric information, even if the information is necessary for the entity to provide its service.

India’s second new privacy rule applies to ISPs. This rule requires ISPs to have privacy policies and terms of use agreements. Terms of use agreements must instruct users to refrain from using the ISP to share information that the user does not own, is pornographic or blasphemous, is harmful to minors, infringes intellectual property rights, misleads another as to the origin of the information, or contains malicious computer code.

APPLICATION TO INTERNET BUSINESS—PRIVACY POLICY CHECKLISTS

General Consumer Websites

In an age of FTC enforcement and class action litigation, virtually every consumer website now posts a privacy policy and terms of use agreement. The FTC routinely holds website operators accountable for their online data practices and ensures their practices match their policies. As a result, the golden rule for the creation of privacy policies and terms of use agreements is to “do what you say” and to “say what you do.” Creating a policy that accurately reflects a website operator’s practices represents an ongoing compliance challenge for many organizations and an important first step to preventing an FTC investigation into a potential unfair and deceptive trade practice.

Financial, Health, EU-Originating, or Children’s Information

Because the U.S. often regulates privacy by sector or industry, organizations can easily overlook laws that may apply to them. When drafting privacy policies, a website operator should become aware of laws that impact how the operator may collect, use, and disclose personal information. Financial, health, and children’s information represent common areas where organizations often make mistakes or take unnecessary risks.

A. Financial and Health Information

Transmitting financial or health information online may subject a website to privacy laws despite the website’s otherwise general focus. For example, credit-card and online profiling information may be considered personal financial information under the GLB Act. Similarly, such information may be stored online for use in determining creditworthiness under the FCRA. Many consumer website operators look closely at the GLB Act’s definition of

684 Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, Gazette of India, part II, section 3(i) (April 11, 2011) [henceforth India Data Rule].
685 Information Technology (Intermediaries Guidelines) Rules, 2011, Gazette of India, part II, section 3(i) (April 11, 2011) [henceforth India ISP Rule].
686 India Data Rule, supra note 684, §§ 3, 5.
687 See India ISP Rule, supra note 685, § 3 (stating the rule applies to an “intermediary,” which, is defined as “any person who on behalf of another person receives, stores or transmits [an electronic] message or provides any service with respect to that message” (No. 21 of 2000, §2(1)(w)).
688 Id. at § 3(1).
689 Id. at § 3(2).
“financial institution” to determine whether the GLB Act’s rigorous notice and consent obligations apply. Moreover, state regulations add more requirements and variations in website policy. Finally, transferring information related to employees may create problems with international privacy law compliance. U.S. corporations may have voluntary programs or legal requirements to track the race, age, disability status, or other “sensitive data” of their employees. Compiling and transferring such data may require express, informed consent from their employees.

B. Children’s Information

To the extent a website targets children or knowingly collects information from children, the website must comply with COPPA. Many general audience websites post the following simple disclaimer to comply with COPPA:

The Operator supports and complies with the Children’s Online Privacy Protection Act. This website is not targeted to children and does not knowingly collect information from children under the age of thirteen, nor do we disclose such information to third parties.

However, a disclaimer may not be enough. Website operators frequently risk running afoul of COPPA if user profile data includes a field for the date of birth, and the website does not automatically reject information received from a user who identifies himself as a child under the age of thirteen. Similarly, if an online form collects information from parents about family members that would identify a child, the website may have COPPA obligations. Finally, while determining whether a website operator has actual knowledge of data collection from children may be straightforward, determining whether a website is directed to children may be more difficult. COPPA provides some examples and guidance, but as a practical matter, many website operators approach the issue conservatively. As discussed above, general audience websites often include disclaimers in their privacy policies. Additionally, many websites use age-neutral screening mechanisms to prevent children from accessing portions of the website where personal information might be collected.

Checklist for a Consumer Privacy Policy

Online privacy policies should be reviewed in connection with the standards of international data collection, especially from the European Union. Common practices for the creation of online privacy policies include the following:

- Describe what information is collected and how it is collected, as well as the intended use and third party recipients of personal information. If information will be disclosed to third parties, reserve this right to the operator. Explicitly state that any actual correspondence, such as e-mails, will be collected and stored.
- Explain that a user may avoid entering profile information and may disable cookies. Inform the user whether disabling cookies will impact the operation of the site. Check to ensure your cookie-disabling technology or process is working at least once a week. The FTC frequently investigates and tests methods of consumer control (such as opt-outs).
- Review the use of technologies that may work similarly to cookies or in conjunction with them and check disclosures relating to the use of such technologies. Increasingly businesses have seen litigation result from the use or deployment of data-collecting technologies in ways that consumers allegedly did not know about or had not agreed to in connection with use of the website or device.


691 See supra text accompanying notes 248-287.

692 See 16 C.F.R. § 312.2.

693 An age-neutral screening system allows a user to freely enter his month, day, and year of birth. A website that only allows users to enter birth years making them 13 or older is not a neutral age-screening mechanism, because children cannot enter their correct age. Federal Trade Commission, Frequently Asked Questions about the Children’s Online Privacy Protection Rule, http://www.ftc.gov/privacy/coppafaqs.shtm.

694 La Court v. Specific Media, Inc., No. SACV 10-1256-GW(JCGx), 2011 WL 2473399 (C.D. Cal. Apr. 28, 2011) (plaintiff failed to establish standing due to failure to allege damage from defendant’s cookie tracking to a specific plaintiff and economic
operators increasingly make specific disclosures regarding the automatic collection, use, and disclosure of information generated from the use of their website for online advertising and other purposes.

- Inform users on how they can view the information collected about them. Often a technological solution works best. Many sites allow users to edit or delete their online profiles, and the policy may explain that deleting cookies will delete most of the information collected about them.

- Explain the steps the website operator takes to secure information during website use or while in storage. FTC enforcement actions suggest that statements regarding security are likely best qualified with disclaimers or other language so as not to create a warranty of privacy or security. The FTC has enforced such implied warranties based on a company’s representations. Whether a disclaimer is effective has not yet been litigated. The routine presence of affirmative security-related statements and the FTC’s enforcement actions suggest websites will increasingly be accountable for data security.

- Require third parties to whom information is disclosed to obey the same privacy principles as the disclosing party. Many security breaches and related issues arise in connection with the use of vendors and suppliers. Data supply chain management represents an on-going challenge, and businesses should place an emphasis on improving in this area.

- Provide a mechanism for users to ask questions or register complaints concerning the collection of personal information.

- Reserve the right to update or alter the privacy policy at any time. This may not be wholly practical on an operations level, however. The FTC has explicitly stated it will review whether consent has been given to changed information practices.

Checklist for Data Security

Website operators must take reasonable steps to ensure the security of the personal information they collect or otherwise risk enforcement actions and litigation. Not only has the FTC issued guidance in this area, but international standards bodies and others are increasingly developing technical benchmarks that are being used to analyze whether or not underlying security measures are reasonable. Compliance with the EU Directive and the DOC’s Safe Harbor provision represents an issue of increasing importance. For example, companies registered under the Safe Harbor must have adequate data security procedures, which include the following:

- Permit individuals to
  - opt out of the collection or use of their personal information,
  - access personally identifiable information collected about them, and
  - correct inaccurate information;

- Do not collect “sensitive data”;

- Require third parties to whom information is disclosed to obey the same privacy principles as the disclosing party by contract;

- Ensure that data are relevant for the purpose for which they are collected; and

- Follow the procedures for enforcement, including dispute resolution.

In general, regulators have made clear that website operators who have no particular need for sensitive personal information should not collect it. In fact, David Vladeck, the Director of the FTC’s Bureau of Consumer Protection, harm from such action). Valdez v. Quantcast Corp., No. CV10-5484 (C.D. Cal. July 23, 2010) (settlement for $2.5 million after Quantcast allegedly tracked people’s online activities using Flash cookies, which could not be deleted by browser settings); Findings of Fact, Conclusions of Law, and Order Approving Settlement, Lane v. Facebook, Inc., No. C 08-3845 RS, 2010 U.S. Dist. LEXIS 24762 (N.D. Cal. Mar. 17, 2010) (settlement for $9 million after its 2007 Beacon marketing program allegedly tracked and published users’ e-commerce activity on non-Facebook websites like Blockbuster and Overstock.com without user knowledge or consent).

695 Cf., Twitter, Inc.; Analysis of Proposed Consent Order to Aid Public Comment, 75 Fed. Reg. 37806 (June 30, 2010); Twitter, Inc., 151 F.T.C. 162, 165 (June 24, 2010) (forming the basis for the FTC’s Section 5 allegations: “Twitter is very concerned about safeguarding the confidentiality of your personally identifiable information. We employ administrative, physical, and electronic measures designed to protect your information from unauthorized access.”).
recently remarked, “If you don’t want to see us, don’t collect data you don’t need.” Companies may include liability waivers in connection with the loss of consumer information to limit exposure to data losses, although the value of such waivers in defending enforcement actions remains uncertain.

CONCLUSION

Internet businesses are constantly innovating and providing new services that benefit users. However, as the services become more useful, they tend to also increase the amount of data collection. The more data an Internet service has about a user, the more the service can be customized to meet the user’s needs. As data is collected, privacy questions arise. Two of the important questions Internet businesses must consider are (1) whether they are transparent about what data they collect, and (2) whether they properly protect the data they collect. Internet business that fail to consider the privacy implications of their data policies risk facing costly litigation and government investigations.

[Last updated December 2012.—Ed.]

__________

[The next page is PR-1.—Ed.]