WILLKIE FARR & GALLAGHER LLP

KEY U.S. DATA PRIVACY & SECURITY REGULATORY DEVELOPMENTS AS OF APRIL 25, 2014

CONGRESS

Topic / Key Words	Bill / Law	Sponsor(s)	Description	Status / Comments
			113TH CONGRESS (2013-2014)	
Biometric Information Privacy	H.R. 4381: Biometric Information Privacy Act	Rep. Stockman (R-TX)	The bill would require business entities and certain other persons to protect the privacy of an individual's "personal physiological biometric information, " defined as: genetic information; finger prints; palm prints; hand geometry; iris scans; retina scans; and eye vein scans.	4/2/14: Introduced and referred to the House Judiciary Committee.
Children's Privacy	H.R. 2645: FACE Act of 2013	Rep. Duncan (R-TN) 2 Cosponsors	The Forbidding Advertisement Through Child Exploitation Act of 2013 (the "FACE Act") would prohibit social media service providers from intentionally or knowingly using for a commercial purpose a self-image uploaded by a minor. A violation would be treated as an unfair or deceptive act or practice under the Federal Trade Commission Act and would be enforced by the FTC or state attorneys general.	7/10/13: Introduced and referred to the House Energy and Commerce Committee.
Children's Privacy	S. 1700: Do Not Track Kids Act	Sen. Markey (D-MA) 2 Cosponsors	This legislation would amend the Children's Online Privacy Protection Act of 1998 to apply the prohibitions against collecting personal information from children to online applications and mobile applications directed to children. It would also establish additional privacy protections against the collection of personal or geolocation information from children and minors.	11/14/13: Introduced and referred to the Senate Committee on Commerce, Science, and Transportation.
Children's Privacy	H.R. 3481: Do Not Track Kids Act	Rep. Barton (R-TX) 33 Cosponsors	This is the House companion bill to Sen. Markey's S. 1700 (above).	11/14/13: Introduced and referred to the House Committee on Energy and Commerce.

CONGRESS (continued)

Cybersecurity	S. 884: Deter Cyber Theft Act	Sen. Levin (D-MI) 3 Cosponsors	This measure would require the Director of National Intelligence to develop watch lists of countries that engage in economic or industrial espionage in cyberspace affecting trade secrets or proprietary information in the United States.	5/7/13: Introduced and referred to the Senate Finance Committee.
Cybersecurity	H.R. 3696: National Cybersecurity and Critical Data Protection Act	Rep. McCaul (R-TX) 3 Cosponsors	This legislation would establish a voluntary structure within which the federal government and the private sector could cooperate to protect U.S. critical infrastructure from cyber attack and operators of critical infrastructure systems could obtain timely technical assistance, crisis management, and recommendations on cyber threats.	12/11/13: Introduced and referred to the House Committee on Homeland Security and other committees. 1/15/14: Approved by the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies.
Data Breach	S. 1897: Personal Data Privacy and Security Act of 2014	Sen. Leahy (D-VT) 5 Cosponsors	Key provisions of the bill would: expand federal criminal prohibitions and penalties for identity theft and other violations of data security and privacy; require the Federal Trade Commission to issue regulations specifying safeguards for the protection of "sensitive personally identifiable information" (as defined by the legislation); require compliance with such regulations and other data security provisions of the Act by any business that involves collecting, accessing, transmitting, using, storing, or disposing of sensitive information in electronic or digital form on 10,000 or more U.S. persons; establish requirements for notifications to consumers of data breaches; and provide an exception from the requirements of this legislation for entities already regulated by the Gramm-Leach-Bliley Act and the Health Insurance Portability and Accountability Act.	1/8/14: Introduced and referred to the Senate Judiciary Committee.
Data Breach	S. 1927: Data Security Act of 2014	Sen. Carper (D-DE) 1 Cosponsor	Key provisions of this measure would: prescribe certain security procedures for an entity that maintains or communicates sensitive account or personal information to protect the information from an unauthorized use likely to result in substantial harm or inconvenience to the consumer; authorize enforcement by specified federal regulatory agencies having oversight of financial institutions; preempt state laws regarding data security breaches; and expressly deny a private right of action, including a class action, regarding any act or practice regulated by this legislation.	1/15/14: Introduced and referred to the Senate Banking, Housing, and Urban Affairs Committee.

CONGRESS (continued)

Data Breach	S. 1976: Data Security and Breach Notification Act of 2014	Sen. Rockefeller (D-WV) 3 Cosponsors	This legislation would: require the Federal Trade Commission to issue regulations requiring covered entities (corporations, partnerships, estates, trusts, and others) that own or possesses personal information to implement policies and procedures regarding information security practices for the treatment and protection of such information; establish procedures for notices of information data breaches that would be provided to the affected individuals as well the federal agencies designated by the legislation; establish requirements regarding the methods and timeliness of the notice; provide an exemption from the notice requirement if the covered entity reasonably concludes that there is no reasonable risk of identity theft, fraud, or other unlawful conduct; and establish a presumption that there is no such risk for encrypted data.	1/30/14: Introduced and referred to the Senate Commerce, Science, and Transportation Committee.
Data Breach	S. 1995: Personal Data Protection and Breach Accountability Act of 2014	Sen. Blumenthal 1 Cosponsor	This legislation would enhance federal criminal penalties for identity theft and other violations of data privacy and security and would criminalize concealment of a security breach involving sensitive personally identifiable information that results in economic harm or substantial emotional distress to one or more persons. It would impose civil fines up to $1 million on a service provider that knowingly or intentionally redirects web searches or otherwise monitors, manipulates, aggregates, and markets data from websites without the consent of the Internet user. In addition, the bill would impose certain data security and date breach notification requirements on an interstate business entity that collects, accesses, transmits, uses, stores, or disposes of sensitive personally identifiable information on 10,000 or more U.S. persons (with certain exceptions). The legislation would permit a private right of action to recover damages for personal injuries sustained as a result of a violation, including punitive damages for intentional or willful violations, or to obtain injunctive relief.	2/4/14: Introduced and referred to the Senate Judiciary Committee.
Data Breach	Senate Hearing	Sen. Warner (D-VA)	The Senate Committee on Banking, Housing and Urban Affairs Subcommittee on National Security and International Trade and Finance held a hearing on 2/13/14, "Safeguarding Consumers' Financial Data." Subcommittee leaders expressed the hope that they could draft a timely legislative response to recent data security breaches at Target Corp. and other retailers provided that the various industry stakeholders cooperate in the effort.	2/3/14: Hearing held.

CONGRESS (continued)				
Data Breach	Senate Hearing	Sen. Leahy (D-VT)	The Senate Judiciary Committee held a hearing on 2/4/14, "Privacy in the Digital Age: Preventing Data Breaches and Combating Cybercrime." Federal Trade Commission Chairwoman Edith Ramirez called for a federal breach notification law to replace the numerous state laws in this area.	2/4/14: Hearing held.
Data Breach	H.R. 3990: Data Privacy and Security Act	Rep. Shea-Porter (D-NH)	This is the House companion measure to Sen. Leahy's S. 1897 (see above).	2/4/14: Introduced and referred to the House Judiciary Committee
Data Breach	H.R. 1121: Cyber Privacy Fortification Act of 2013	Rep. Conyers (D-MI) 2 Cosponsors	The bill would require a person who owns, possesses, or maintains sensitive personally identifiable data in electronic form, and who has knowledge of a major security breach of the system containing such data, to report the security breach to the U.S. Secret Service or the Federal Bureau of Investigation. The measure would also establish federal criminal penalties for intentional failure to provide the required notice.	3/13/13: Introduced and referred to the House Judiciary Committee.
Data Breach	Senate Hearing	Sen. Rockefeller (D-WV)	The Senate Commerce, Science and Transportation Committee held a hearing on March 26, 2014 on "Protecting Personal Consumer Information from Cyber Attacks and Data Breaches." The hearing focused on the recent, high-profile data breach at Target, and less-reported breaches at entities such as Neiman Marcus, White Lodging, Snapchat, and the University of Maryland, which committee leaders believe have highlighted the need for congressional action to improve the protection of consumer data. In advance of the hearing, Committee Chairman Rockefeller released a report charging that Target failed to take adequate steps to prevent a breach of its payment card system. The report also asserted that Target missed opportunities to detect and stop the hacking, including multiple warnings by the company's antiintrusion software.	3/26/14: Hearing held and report released.

CONGRESS (continued)				
Data Breach	H.R. 4400: Data Accountability and Trust Act	Rep. Rush (D-IL) 5 Cosponsors	The legislation would direct the Federal Trade Commission to issue regulations requiring each person engaged in interstate commerce that owns or possesses data containing personal information, or contracts with a third party to maintain such data, to establish and implement policies and procedures regarding information security practices for the treatment and protection of personal information and establishing procedures for notification regarding data breaches to affected individuals. These provisions would apply only to persons or entities over which the FTC already has authority. The bill would also establish a regime for the regulation of "information brokers" (as defined) and require FTC rulemaking to implement the regime.	4/4/14: Introduced and referred to the House Energy and Commerce Committee.
Data Brokers		Senate Commerce, Science, and Transportation Committee – Congressional Inquiry	In October 2012, the Senate Commerce Committee began an inquiry into the practices of data brokers by writing to nine large data brokers to obtain information that would help determine the impact of such practices on consumers. In September 2013, Chairman Rockefeller expanded the investigation by writing to 12 popular health and personal finance websites with questions about their data collection and sharing practices and noting that several data brokers had refused to disclose to the Committee specific sources of consumer data and, in his view, had prevented the Committee from fully understanding how the industry operates. In December 2013, the Committee released a staff report entitled *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes*. In February 2014, Chairman Rockefeller and Sen. Markey introduced the Data Broker Accountability and Transparency Act of 2014 (the "DATA Act") to require data brokers "to be accountable and transparent about the information they collect and sell about consumers." See entry on S. 2025.	10/9/12: Chairman Rockefeller sends initial round of letters to selected data brokers. 9/24/13: Chairman Rockefeller writes to an additional 12 data brokers. 12/18/13: Committee staff report on data brokers released. 2/12/14: S. 2025 introduced.

CONGRESS (continued)

Data Brokers	S. 2025: Data Broker Accountability and Transparency Act	Sen. Rockefeller (D-WV) 1 Cosponsor	The legislation would define "data broker" and establish a regulatory regime for data brokers that would include: requirements for data brokers to ensure the accuracy of the personal information they collect, assemble, or maintain; access by individuals to the information collected or maintained about them by a data broker; and the opportunity for individuals to express a preference as to the use of their personal information for marketing purposes.	2/12/14: Bill introduced and referred to the Senate Committee on Commerce, Science and Transportation.
Drones	S. 1057: Safeguarding Privacy and Fostering Aerospace Innovation Act of 2013	Sen. Udall (D-CO)	This legislation would prohibit the use of unmanned aircraft systems by private persons to conduct surveillance of other private persons. It would require the owner of a civil unmanned aircraft system to clearly mark the aircraft with the owner's name and contact information.	5/23/13: Introduced and referred to the Senate Judiciary Committee.
Drones	H.R. 637: Preserving American Privacy Act of 2013	Rep. Poe (R-TX) 34 Cosponsors	H.R. 637 would provide a legal framework for the operation of public unmanned aircraft systems by a governmental entity to minimize the collection or disclosure of information reasonably likely to enable identification of an individual or information about an individual's property that is not in plain view.	2/13/13: Introduced and referred to the House Judiciary Committee.
Drones	H.R. 1262: Drone Aircraft Privacy and Transparency Act of 2013	Rep. Markey (D-MA) 1 Cosponsor	This bill would amend the FAA Modernization and Reform Act of 2012 to direct the U.S. Department of Transportation (DOT) to study and identify potential threats to privacy posed by the integration of unmanned aircraft (drone) systems into the national airspace system and to ensure that integration of drone systems into the national airspace system complies with privacy principles. Applicants for a license to operate a drone system in the national airspace system must provide a data collection statement meeting certain requirements and providing reasonable assurance that the system will operate in accordance with privacy principles. The measure would make it unlawful to operate a drone system in a manner that violates the terms of a data collection statement and grants enforcement authority to the Federal Trade Commission (FTC), while also authorizing state civil actions and private rights of action to enforce the provisions of this measure. Note: On 7/16/13, Rep. Markey departed the House of Representatives and became a member of the U.S. Senate.	3/19/13: Introduced and referred to the House Energy and Commerce Committee.

CONGRESS (continued)

Drones	H.R. 2868: Drone Aircraft Privacy and Transparency Act of 2013	Rep. Welch (D-VT) 4 Cosponsors	This legislation would require that: (1) an application for a drone license from the FAA include a data collection statement meeting certain requirements; (2) a law enforcement agency obtain a warrant for the use of drones in most situations; and (3) the FAA create a website listing approved licenses, data collection statements, data security breaches by a licensee, and the times and locations of flights.	7/30/13: Introduced and referred to the House Energy and Commerce Committee and the Transportation and Infrastructure Committee.
Drones	S. 1639: Drone Aircraft Privacy and Transparency Act of 2013	Sen. Markey (D-MA)	This measure is the same as H.R. 1262, introduced earlier in 2013 by Sen. Markey when he was a member of the House of Representatives (see above).	11/4/2013: Introduced and referred to the Senate Committee on Commerce, Science, and Transportation.
Electronic Communications Privacy Act	S. 607: Electronic Communications Privacy Act Amendments of 2013	Sen. Leahy (D-VT) 4 Cosponsors	S. 607 would require the government to obtain a search warrant to obtain the content of emails and other electronic communications stored with third-party service providers. It would also eliminate the "180-day" rule in current law that provides different legal standards for the government's obtaining email content based on the age of an email and require the government to notify an individual whose electronic communications have been disclosed within 10 days of obtaining a search warrant.	3/19/13: Introduced and referred to the Senate Judiciary Committee. 4/25/13: Ordered favorably reported by the Senate Judiciary Committee by voice vote. 5/16/13: Senate Judiciary Committee report filed, S. Rep. No. 113-34.
Electronic Communications Privacy Act	H.R. 983: Online Communications and Geolocation Protection Act	Rep. Lofgren 18 Cosponsors	The bill is similar to Sen. Leahy's bill (S. 607) above and is intended to reform ECPA.	3/6/13: Introduced and referred to the House Judiciary Committee.
Electronic Communications Privacy Act	H.R. 1847: Electronic Communications Privacy Act Amendments of 2013.	Rep. Salmon (R-AZ) 24 Cosponsors	H.R. 1847 is identical to Sen. Leahy's bill (S. 607) above and is intended to reform ECPA.	5/7/13: Introduced and referred to the House Judiciary Committee.
Electronic Communications Privacy Act	H.R. 1852: Email Privacy Act	Rep. Yoder (R-KS) 182 Cosponsors	H.R. 1852 is identical to the Leahy, Salmon, and Lofgren bills above and is intended to reform ECPA.	5/7/13: Introduced and referred to the House Judiciary Committee.

CONGRESS (continued)

Employee Privacy	S. 1426: Password Protection Act of 2013	Sen. Blumenthal (D-CT) 6 Cosponsors	S. 1426 would prohibit an employer or prospective employer from compelling or coercing access to an individual's password-protected accounts but would preserve the rights of employers to control access to their own hardware, as well as any Internet software operated on behalf of the employer for work purposes.	8/1/13: Introduced and referred to the Senate Health, Education, Labor, and Pensions Committee.
Financial Privacy	H.R. 2571: Consumer Right to Financial Privacy Act of 2013	Rep. Duffy (R-WI) 7 Cosponsors	H.R. 2571 would amend the Dodd-Frank Wall Street Reform and Consumer Protection Act to prohibit the Consumer Financial Protection Bureau (CFPB) from requesting, accessing, collecting, using, retaining, or disclosing nonpublic personal information about a consumer without the consumer's consent.	6/28/13: Introduced and referred to the House Financial Services Committee. 2/6/14: Committee issues H. Rept. 113-344; bill placed on House Calendar.
Government Surveillance Authority	S. 1121: Fourth Amendment Restoration Act	Sen. Paul (R-KY)	This bill states that the Fourth Amendment to the U.S. Constitution shall not be construed to allow any agency of the United States Government to search the phone records of Americans without a warrant based on probable cause.	6/7/13: Introduced. 6/10/13: Bill placed on Senate Calendar.
Government Surveillance Authority	S. 1130 / H.R. 2475: Ending Secret Law Act	Sen. Merkley (D-OR / Rep. Schiff (D-CA) 15 Cosponsors of S. 1130 30 Cosponsors of H.R. 2475	This legislation would require the Attorney General to disclose certain decisions, orders, or opinions of a FISA court unless such disclosure is not in the United States' national security interest.	6/11/13: S. 1130 introduced and referred to the Senate Judiciary Committee. 6/20/13: H.R. 2475 introduced and referred to the House Judiciary Committee and the House Select Intelligence Committee.
Government Surveillance Authority	S. 1168: Restore Our Privacy Act	Sen. Sanders (I-VT)	S. 1168 would amend the Foreign Intelligence Surveillance Act ("FISA") to limit overbroad surveillance requests by the federal government and to expand requirements for the government's reporting of its activities under FISA. It would also amend the "business records" provision of the USA PATRIOT Act (the "PATRIOT Act") to require the federal government to provide specific evidence to justify reasonable suspicion before obtaining court approval to monitor business records related to a specific terrorism suspect.	6/13/13: Introduced and referred to the Senate Judiciary Committee.

CONGRESS (continued)				
Government Surveillance Authority	S. 1182	Sen. Udall (D-CO) 8 Cosponsors	Informally referred to by its sponsors as the "Nexus to Terrorism Act," the bill would limit the federal government's ability to collect data on U.S. citizens who have no links to terrorism or espionage. It would amend FISA to require specific evidence for access to business records and "other tangible things."	6/18/13: Introduced and referred to the Senate Judiciary Committee.
Government Surveillance Authority	S. 1215: FISA Accountability and Privacy Protection Act of 2013	Sen. Leahy (D-VT) 10 Cosponsors	This legislation would amend the USA PATRIOT Act and FISA by: (1) raising the standards for the federal government's use of the surveillance authorities in these statutes; (2) requiring increased transparency, including public reporting, of the government's use of such authorities; and (3) providing increased judicial review of the government's activities in this area, especially when surveillance of a U.S. person is involved, and greater oversight by the Inspector General of the Intelligence Community.	6/24/13: Introduced and referred to the Senate Judiciary Committee.
Government Surveillance Authority	S. 1467: FISA Court Reform Act of 2013	Sen. Blumenthal (D-CT) 18 Cosponsors	S. 1467 would establish the Office of Special Advocate with authority to act as "opposing counsel" to challenge federal government requests for surveillance orders or directives under FISA and to represent the right to privacy and other individual rights in the FISA Court.	8/1/13: Introduced and referred to the Senate Judiciary Committee.
Government Surveillance Authority	Senate Letter	Sen. Leahy (D-VT) and 8 other Senators	On 9/23/13, Senate Judiciary Committee Chairman Leahy (D-VT), Committee Ranking Member Grassley (R-IA) and seven other Senators wrote to the Inspector General ("IG") of the Intelligence Community asking the IG to review the use of federal surveillance authorities and to make the findings public. Specifically, the Senators requested detailed information on the surveillance of U.S. citizens conducted pursuant to FISA and the USA PATRIOT authorities and any misuse of such authority during the last three years, stating that a "publicly available summary of the findings and conclusions of these reviews will help promote greater oversight, transparency, and public accountability."	9/23/13: Letter sent to the IG.
Government Surveillance Authority	S. 1551: Intelligence Oversight and Surveillance Reform Act	Sen. Wyden (D-OR) 13 Cosponsors	This bill would amend FISA and other national security statutes to prohibit bulk collection by the federal government of domestic communications, e.g., phone records. In addition, the legislation would create an independent "Constitutional Advocate" to act as opposing counsel against the government in significant matters before the FISA Court.	9/25/13: Introduced and referred to the Senate Judiciary Committee.
Government	H.R. 2399:	Rep. Conyers (D-MI)	The Limiting Internet and Blanket Electronic Review of Telecommunications and Email Act ("LIBERT-E Act") would restrict the	6/17/13: Introduced and referred to the House

CONGRESS (continued)				
Surveillance Authority	LIBERT-E Act	53 Cosponsors	federal government's ability to collect information on U.S. citizens who are not connected to ongoing antiterrorism or intelligence investigations. It would also require that court opinions issued pursuant to FISA be provided to Congress and that summaries of the opinions be made public.	Judiciary Committee and the House Select Intelligence Committee.
Government Surveillance Authority	H.R. 2440: FISA Court in the Sunshine Act of 2013	Rep. Jackson-Lee (D-TX) 12 Cosponsors	This legislation would require the Attorney General to disclose certain decisions, orders, or opinions of a FISA court unless such disclosure is not in the United States' national security interest.	6/19/13: Introduced and referred to the House Judiciary Committee and the House Select Intelligence Committee.
Government Surveillance Authority	H.R. 2586	Rep. Cohen (D-TN) 11 Cosponsors	The bill would amend FISA to provide for the designation of Foreign Intelligence Surveillance Court judges by the Speaker of the House of Representatives, the minority leader of the House of Representatives, the majority and minority leaders of the Senate, and the Chief Justice of the United States.	6/28/13: Introduced and referred to the House Judiciary Committee and the House Select Intelligence Committee.
Government Surveillance Authority	H.R. 2603: Relevancy Act	Rep. Ross (R-FL)	The legislation would amend FISA to permit federal government access, for antiterrorism or intelligence purposes, to certain business records only if an investigation specifically relates to the individual or group of individuals whose records are the target of the government's inquiry.	6/28/13: Introduced and referred to the House Judiciary Committee and the House Select Intelligence Committee.
Government Surveillance Authority	H.R. 2849: Privacy Advocate General Act of 2013	Rep. Lynch (D-MA) 1 Cosponsor	H.R. 2849 would amend FISA to, among other things, establish the Office of the Privacy Advocate General as an independent office in the executive branch, to be headed by a Privacy Advocate General appointed jointly by the Chief Justice of the United States and the senior Associate Justice for a seven-year term. The Privacy Advocate General would act as "opposing counsel" regarding federal government requests for an order or directive under FISA and any certification or targeting procedures and argue the merits of the opposition before the FISA court.	7/30/13: Introduced and referred to the House Judiciary Committee and the House Select Intelligence Committee.

CONGRESS (continued)				
Gramm-Leach-Bliley Financial Privacy	S. 635	Sen. Brown (D-OH) 48 Cosponsors	This measure would amend the Gramm-Leach-Bliley Act to provide an exception to the annual written privacy notice requirement for financial institutions if a financial institution's privacy policy and procedures have not changed since the last annual notice.	3/21/13: Introduced and referred to the Senate Banking, Housing and Urban Affairs Committee.
Gramm-Leach-Bliley Financial Privacy	H.R. 749: Eliminate Privacy Confusion Act	Rep. Luetkemeyer (R-MO) 73 Cosponsors	H.R. 749 would amend the Gramm-Leach-Bliley Act to provide an exception to the annual written privacy notice requirement for financial institutions if a financial institution's privacy policy and procedures have not changed since the last annual notice.	2/15/13: Introduced and referred to the House Financial Services Committee. 3/12/13: Passed the House under suspension of the rules (two-thirds vote required) by voice vote. 3/13/13: Received in the Senate and referred to the Senate Banking, Housing and Urban Affairs Committee.
Mobile Device Privacy	H.R. 210	Rep. Serrano (D-NY)	H.R. 210 would require retail establishments that use mobile device tracking technology to display notices to that effect.	1/4/13: Introduced and referred to the House Energy and Commerce Committee.
Mobile Device Privacy	H.R. 1913: Application Privacy, Protection and Security (APPS) Act of 2013	Rep. Johnson (D-GA) 6 Cosponsors	The bill is intended to provide for greater transparency in, and user control over, the treatment of data collected by mobile applications and to enhance the security of such data.	5/9/13: Introduced and referred to the House Energy and Commerce Committee.

FEDERAL AGENCIES

Topic / Key Words	Agency	Action	Description	Status / Comments
Children's Online Privacy Protection Act ("COPPA")	Federal Trade Commission ("FTC")	Revised Rule Released Enforcement Team Changes Divisions FAQs Released Informational Letters Sent FTC Approved Safe Harbor Program FTC Approved Method to Verify Parental Consent Comment Sought on Proposed Safe Harbor Program Updated FAQs Posted	On 12/19/12, the FTC announced the adoption of comprehensive amendments to the Children's Online Privacy Protection Rule (the "Rule"), which implements the 1998 Children's Online Privacy Protection Act ("COPPA"). The revised Rule went into effect on 7/1/13. Some of the adopted amendments include: • Expanding the definition of "personal information" to include "persistent identifiers" (e.g., IP addresses, unique device identifiers, etc.) in certain situations; photos, videos, and audio files that include a child's image or voice; and geolocation information; • Defining the term "support for internal operations" to include contextual advertising, legal compliance, site analysis, security and integrity, and network communications, and providing a mechanism to have additional activities included in the definition moving forward (the revised Rule allows sites to collect persistent identifiers without notice and parental consent if the collection is necessary to support internal operations); • Establishing that child-directed sites or services are strictly liable for the COPPA compliance of any third-party services, such as ad networks and social networking plug-ins, that collect personal information through the child-directed site or service; • Expanding the scope of COPPA to include third-party service providers that have "actual knowledge" that they are collecting personal information through a child-directed site or service; • Permitting "child-directed" sites and services that do not target children as their primary audience to age screen users, and only requiring notice and parental consent for users that self-identify as under 13; • Establishing data retention and data security requirements, including for data that is "released" to third parties; and • Expanding the list of acceptable methods to obtain parental consent. On 4/25/13, the FTC released updated FAQs as guidance to help interested parties understand the FTC's COPPA Rule changes. On 5/15/13, the FTC sent more than 90 "educational letters" regarding the	9/27/11: Notice of Proposed Rulemaking released. 8/1/12: Supplemental Notice of Proposed Rulemaking released. 12/19/12: Revised COPPA Rule released. 2/20/13: Announcement of division change for COPPA enforcement. 4/25/13: FAQs released. 5/6/13: FTC voted to retain implementation date. 5/15/13: Informational letters sent. 7/1/13: Revised COPPA Rules went into effect. 8/15/13: Comments sought on AssertID Inc.

			COPPA Rule changes to four types of mobile app developers: (1) domestic companies that may be collecting images or sounds of children; (2) domestic companies that may be collecting persistent identifiers from children; (3) foreign companies that may be collecting images or sounds of children; and (4) foreign companies that may be collecting persistent identifiers from children. On 8/15/13, the FTC sought public comment on a proposal from AssertID Inc. to approve a new method of verifying parental consent. The COPPA Rule allows interested parties to submit new verifiable parental consent methods to the FTC for approval. Comments were due 9/20/13. Commenters urged the FTC to reject AssertID's proposal. The Center for Digital Democracy claimed that the proposed verified consent mechanism will harm consumers by requiring parents to divulge their personal information and that AssertID left important parts of the consent process unexplained. On 11/13/13, the FTC denied AssertID's application for failing to provide sufficient evidence demonstrating that its proposed parental consent method is reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent. On 9/12/13, the FTC sought public comment on a proposal from Imperium LLC to approve a new method of verifying parental consent. Comments were due 10/9/13. On 12/23/13, the FTC announced it approved Imperium's method of verifying parental consent. On 9/16/13, the FTC sought comment on a proposal by Samet Privacy for the FTC to adopt Samet's kidSAFE Seal Program as a COPPA safe harbor program. Five other groups have previously received approval for safe harbor programs: the Children's Advertising Review Unit of the Council of Better Business Bureaus, the Entertainment Software Rating Board, TrustE, Privo Inc., and Aristotle International Inc. Comments on Samet's proposal were due on 10/18/13. On 2/12/14, the FTC announced it approved the kidSAFE Seal Program as the first COPPA safe harbor program adopted under the new rule. On 2/25/14, the FTC announced it concluded that it was unnecessary to approve a verifiable parental consent method under COPPA proposed by iVeriFly Inc. The FTC stated that iVeriFly's VPC method is a variation on verifiable parental consent methods already recognized in the COPPA Rule or recently approved by the FTC and thus did not require specific approval by the FTC. The iVeriFly method involves verifying a parent's social security number or by setting verification codes. On 3/13/14, the FTC announced that it is seeking public comment on a COPPA Safe Harbor program proposed by the Internet Keep Safe Coalition (iKeepSafe). On 4/23/14, the FTC posted updated COPPA FAQs on COPPA's application to	proposal. 9/12/13: Comments sought on Imperium LLC proposal. 9/16/13: Comments sought on kidSAFE Seal Program. 9/20/13: Comments due on AssertID Inc. proposal. 10/9/13: Comments due on Imperium LLC proposal. 10/18/13: Comments due on kidSAFE Seal Program. 11/13/13: FTC denied AssertID's application. 2/12/14: FTC approved kidSAFE Seal Program as COPPA safe harbor. 2/25/14: FTC announced approval for parental consent method. 3/13/14: Comment sought on iKeepSafe safe harbor

			schools. The FAQs seek to provide guidance and best practices for apps and websites providing educational tools to children while in school.	program. 4/23/14: Updated FAQs posted.
Cybersecurity	White House National Institute of Standards and Technology ("NIST") Department of Commerce ("DOC") Department of Homeland Security ("DHS") Department of Treasury Department of Defense ("DoD") General Services Administration ("GSA")	Executive Order Released Reports Released First Draft of Cybersecurity Framework Released National Governors Association Paper Released Recommendations Issued Voluntary Framework Released	On 2/12/13, the White House released an Executive Order putting in place measures to encourage information sharing between the government and private industry, and establishing voluntary cybersecurity standards for critical infrastructure. The Executive Order requires the government to share unclassified cyber threat information with private industry. This measure does not require private entities to share information with the government. The Executive Order creates unclassified reports of cyber threats that identify a specific targeted entity and a process for disseminating these reports to those entities. The Executive Order requires that the instructions for the creation of these reports be issued within 120 days of the Executive Order. The Executive Order also requires the expansion of the Enhanced Cybersecurity Services (ECS) program for providing classified cyber threat indicators to critical infrastructure companies and their service providers, instead of disseminating the information only to defense contractors. The procedures for this program must also be established within 120 days. In addition, the Executive Order mandates a set of measures aimed at creating voluntary cybersecurity standards for private critical infrastructure owners, including a framework to reduce cyber risks to critical infrastructure. The framework will be developed by NIST in consultation with the National Security Agency and private industry. The framework must include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks. The framework must incorporate voluntary consensus standards and industry best practices. A preliminary version must be established within 240 days for comment, and the final version must be published within one year. On 2/26/13, NIST released a Request for Information soliciting comments on how to structure the framework to achieve the desired result of reducing cyber risks to critical infrastructure. Comments were due 4/8/13. On 8/6/13, the White House unveiled reports from the Department of Commerce ("DOC"), the Department of Homeland Security ("DHS"), and the Department of Treasury recommending incentives to encourage participation from the private sector to adopt cybersecurity best practices for providers of critical infrastructure. The reports provide a variety of recommendations, including: (i) streamlining existing cybersecurity regulations; (ii) offering cybersecurity litigation benefits; (iii) requiring participation in the program as a condition or as a weighted criteria for federal critical infrastructure grants; and (iv) identifying areas where research and	2/12/13: Executive Order released. 2/26/13: Request for information released. 4/3/13: First cybersecurity framework workshop held in Washington, DC. 4/8/13: RFI Comments due. 5/29-31/13: Second cybersecurity framework workshop held in Pittsburgh. 7/10-12/13: Third cybersecurity framework workshop held in San Diego. 8/6/13: Reports released. 8/28/13: First draft of framework released. 9/11-13/13: Fourth cybersecurity workshop held in Dallas. 9/26/13: National Governors

			development can help meet pressing cybersecurity challenges. On 8/28/13, NIST released the first draft of the cybersecurity framework. The draft, titled "Discussion Draft of the Preliminary Cybersecurity Framework," outlines four core cybersecurity functions: identify, protect, detect, and respond. The release of the draft came two weeks before a workshop on 9/11/13 in Dallas where the draft was discussed. An edited draft is expected to be released in October. A final framework must be produced by February 2014. On 9/26/13, the National Governors Association released a paper highlighting the role of states in the country's cybersecurity framework. The paper highlights states' roles in ensuring security of state-owned assets and personally identifiable information such as tax records, driver's licenses, and birth records. On 10/22/13, NIST released its official Preliminary Cybersecurity Framework. On 10/29/13, NIST opened up a 45-day comment period on the framework, which ended on 12/13/13. On 1/29/14, DoD and GSA recommended new ways to better align cyber risk management and acquisition processes in the federal government. The report's recommendations focus on exposure to cyber risks related to acquisitions of information and communications technology. The recommendations were made under a working group from the two agencies established under President Obama's cybersecurity executive order. On 2/12/14, NIST issued the final version of a voluntary framework designed to arm the private sector against mounting cyberthreats. It consists of cybersecurity standards that can be customized to various sectors and adapted by both large and small organizations.	Association paper released. 10/22/13: NIST preliminary framework released. 10/29/13: NIST preliminary framework comment period opened. 12/13/13: NIST preliminary framework comments due. 1/29/14: Recommendations issued. 2/12/2014: Final framework released.
Cybersecurity	DHS	Report Released	On 11/4/13, DHS's inspector general released a report setting forth recommendations for better coordinating the federal government's five cyber operations centers. The report recommends that DHS: (i) collaborate with DoD and NIST to develop a standard set of incident categories to foster information sharing among all federal cyber operations centers; (ii) add more staff to execute the Industrial Control Systems Cyber Emergency Response Team's mission to provide full coverage on the operations floors; (iii) increase the number of analysts available at the National Cybersecurity and Communications Integration Center ("NCCIC"); (iv) include new qualifications and standards of NCCIC personnel; (v) update the National protection and Programs Directorate's Continuity of Operations ("COOP") plan to reflect the current operational structure of its subcomponents; (vi) include a risk	11/4/13: Report released.

			management process of continuity plans; and (vii) finalize the Office of Cybersecurity and Communications COOP plan to reflect the recent alignment and test the plan to ensure that component personnel understand their roles.	
Data Privacy PATRIOT Act	National Security Agency ("NSA") Department of Justice ("DOJ") Federal Bureau of Investigation ("FBI") White House	Government Surveillance Reported White Paper Released Release of Aggregate Data Announced Response to Motions Filed PCLOB Report Issued Notice Filed Petitions Dismissed Fact Sheet Released	On 6/6/13, various news outlets began reporting on a story first run in *The Guardian* that the NSA maintained surveillance over three major telephone networks, as well as various tech companies to help thwart terrorism. The NSA monitored Americans by examining the phone records of customers from Verizon, AT&T, and Sprint Nextel. Under a separate surveillance program, named PRISM, the NSA can search confidential customer data from Microsoft, Yahoo, Apple, Google, Facebook, Skype, AOL, and YouTube. In response to the reporting, Microsoft, Apple, Facebook, and Yahoo released statistics of NSA usage to reassure their customers. On 6/11/13, Google asked DOJ and the FBI for permission to disclose aggregate numbers of its national security requests, including FISA disclosures, in terms of the number that Google receives and the requests' scope. Microsoft, Yahoo, LinkedIn, and Facebook filed separate petitions asking for the same relief. On 8/7/13, the Foreign Intelligence Surveillance Court ("FISC") granted DOJ's request to extend the deadline for it to respond to the petitions from Google, Microsoft, and Facebook. On 8/9/13, the White House released a white paper that defends the administration's broad interpretation of Section 215 of the PATRIOT Act to justify the bulk collection of U.S. phone customer records. On 8/29/13, the Obama administration announced it would publish aggregate data on surveillance orders imposed on U.S. businesses for national security purposes. On 9/30/13, DOJ asked the Foreign Intelligence Surveillance Court to deny the motions filed by Google, Facebook, Microsoft, Yahoo, and LinkedIn. A reply brief is due by 10/21/13. On 12/18/13, the White House released a report from an independent panel on how to overhaul U.S. surveillance policies. The report provides more than 40 recommendations, although the White House has not committed to taking action on any of the proposals. The panel's recommendations included: (i) enacting legislation to terminate the storage of bulk telephone metadata by the government and replace it with a system where private providers hold the information; (ii) adopting a policy that prohibits	6/6/13: Government surveillance programs reported. 8/9/13: White paper released by White House. 8/29/13: Release of aggregate data on surveillance order announced. 9/30/13: Response to motions filed. 10/21/13: Reply brief due. 12/20/13: AT&T and Verizon announce transparency reports. 1/23/14: PCLOB issues report. 1/27/14: Notice filed. 1/27/14: Petitions dismissed. 3/27/14: Fact sheet released.

			the government in any way from subverting, undermining, weakening, or making vulnerable generally available commercial software; (iii) creating a privacy and civil liberties policy official located within the White House national security staff and OMB; and (iv) making the director of NSA a Senate-confirmed position. On 12/20/13, AT&T and Verizon announced plans to publish online semiannual transparency reports providing information about how many law enforcement requests for customer data they received in 2013 from governments in the U.S. and elsewhere. On 1/14/14, at a Senate Judiciary Committee hearing several lawmakers raised concerns over the private sector retaining certain U.S. phone customers' records for national security purposes. On 1/23/14, the Privacy and Civil Liberties Oversight Board ("PCLOB") concluded that NSA's bulk collection of phone data is unlawful. PCLOB stated that the NSA's bulk collection is not justified under Section 215 of the USA PATRIOT Act and has violated ECPA. PCLOB also opposed the idea of having a private third party hold the phone records, instead of the federal government. On 1/27/14, DOJ filed a notice in FISC allowing Internet companies, like Google, Microsoft, and Facebook, to publish certain limited aggregate information on national security orders to provide customer data. DOJ's notice said it would treat these disclosures as no longer prohibited. The notice resolved petitions filed by the tech companies to publish general aggregated surveillance statistics. See "Industry Developments" section below for more details. On 3/27/14, the White House released a fact sheet of President Obama's legislative proposal to end the bulk telephone metadata collection program under Section 215 of the USA PATRIOT Act and instead allow records to remain at telephone companies for the statutory data retention period. The proposal would require the federal government to obtain an individual court order from FISC before reviewing the metadata retained by the phone companies.	
Data Privacy	Government Accountability Office ("GAO")	Report Issued	On 11/15/13, GAO issued a report stating that there are gaps in the U.S.'s statutory privacy framework and that the framework does not always reflect the Fair Information Practice Principles. GAO continued that the "current framework does not fully address changes in technology and marketplace practices that fundamentally have altered the nature and extent to which personal information is being shared with third parties." The GAO recommended that Congress consider taking steps to strengthen the current framework and bring it in line with current practices of collecting and	11/15/13: Report issued.

			sharing personal information.	
Data Privacy Biometric Data	NTIA	New Multistakeholder Process Announced Meetings Held	On 12/3/13, NTIA announced that it would launch a new privacy multistakeholder process on commercial use of facial recognition technology. The announcement said the process would include discussion of the privacy risks associated with the use of photo databases in stores and other commercial settings and face prints as a unique biometric identifier. Meetings were held on 2/6/14, 2/25/14, 3/25/14, and 4/8/14. Additional meetings are planned for 4/29/14, 5/20/14, 6/3/14, and 6/24/14. In 2012, the FTC released a staff report on facial recognition technologies.	12/3/13: New multistakeholder process announced. 2/6/14, 2/25/14, 3/25/14, and 4/8/14: Meetings held.
Data Privacy Data Security	FTC	Final Order Approved *In re Goldenshores Technologies, LLC*, File No. 132 3087 (12/5/13)	On 12/5/13, the FTC released its proposed administrative consent order to settle FTC charges against an app developer that failed to disclose to consumers that its app transmitted geolocation information and device identifiers to third parties even though it was a flashlight application. The settlement requires Goldenshores Technologies, LLC to provide just-in-time notice to consumers explaining how their geolocation information is being collected, used, and shared, and it requires Goldenshores to obtain affirmative express consent before collecting and sharing geolocation information. On 4/9/14, the FTC approved the final order.	12/5/13: Proposed administrative consent order released. 4/9/14: Final order approved.
Data Privacy Data Security	FTC	Spring Seminars Announced Mobile Device Tracking Seminar Held Alternative Scoring Products Seminar Held	On 12/2/13, the FTC announced it will hold a series of spring seminars on alternative scoring products (*i.e.*, the use of predictive scoring to determine consumers' access to products and offers), mobile device tracking, and consumer-generated and controlled health data. The FTC sought to have these seminars because of their importance to consumer privacy. On 2/19/14, the FTC held the seminar on mobile device tracking by retailers. The seminar discussed the proposed Code of Conduct developed by the Future of Privacy Forum and several location analytics companies. The Code of Conduct requires providing an opt-out mechanism and in-store signage of mobile device tracking and the opt-out mechanism. At the seminar, it was disclosed that the vast majority of the retail industry does not support moving forward with a Code of Conduct at this time. On 3/19/14, the FTC held a seminar on alternative scoring products used by many data brokers to predict trends and consumer behavior in a variety of contexts, ranging from identity verification and fraud prevention to marketing and advertising. Consumers have little knowledge of and little access to the underlying	12/2/13: Spring seminars announced. 2/19/14: Mobile device tracking seminar held. 3/19/14: Alternative scoring products seminar held.

			data that comprises these scores. As a result, the FTC raised a variety of potential privacy concerns and questions during the seminar.	
Data Privacy	GAO	Report Released	On 1/6/14, the GAO released a report stating that companies that provide in-car location-based services have taken some steps to protect consumer privacy, but that in many cases their privacy practices are unclear and may place consumers at risk. The report examined the privacy practices of ten selected companies that collect location data to provide in-car location-based services, like General Motors, TomTom, and Google. The report states that clear disclosures are needed on how the companies collect, protect, and share the location data. The GAO issued the report in response to a request from Senator Al Franken (D-MN).	1/6/14: Report released.
Data Privacy	DOC	Report Released	On 1/14/14, DOC's International Trade Administration released a document titled "Key Points Concerning the Benefits, Oversight, and Enforcement of Safe Harbor." The document stated that the U.S.-EU and U.S.-Swiss Safe Harbor Frameworks significantly benefit the U.S., EU, and Swiss economies.	1/14/14: Report released.
Data Privacy	FTC	Settlements Announced	On 1/21/14, the FTC announced it had reached settlements with twelve companies for falsely claiming they were in compliance with the U.S.-EU and U.S.-Swiss Safe Harbor programs. Each settlement is a no-fault consent order for claiming to be in compliance with the Safe Harbor programs when the companies had let their certifications lapse. The twelve companies are: Apperian Inc., Atlanta Falcons Football Club LLC, Baker Tilly Virchow Krause LLP, BitTorrent Inc., Charles River Laboratories International Inc., DataMotion Inc., DDC Laboratories Inc., Level 3 Communications LLC, PDB Sports Ltd., Reynolds Consumer Products Inc., Receivable Management Services Corp., and Tennessee Football Inc.	1/21/14: Settlements announced.
Data Privacy	FTC	Consent Order Proposed	On 2/11/14, the FTC announced it accepted a proposed settlement from Fantage.com to resolve the FTC's complaint that Fantage.com falsely claimed in its privacy policy that it held a current certification under the U.S.-EU Safe Harbor program. Fantage.com failed to renew its certification when it expired in June 2012. The settlement prohibits future misrepresentations by Fantage.	2/11/14: Consent order proposed.
Data Privacy Data Security	White House	Review Begins Letter Sent Public Comment	On 1/23/14, the White House began a 90-day review of privacy issues surrounding public and private sector uses of big data. President Obama announced the big data review as part of his 1/17/14 speech addressing concerns	1/23/14: Review begins. 2/10/14: Letter

		Sought	about the NSA's surveillance activities. On 2/10/14, a coalition of privacy groups sent a letter to the White House asking for a public comment period to be included its review. On 3/4/14, the White House announced it is seeking public comment on the adequacy of consumer privacy laws in light of big data trends in the government and private sector. Comments were due 3/31/14.	sent. 3/4/14: Public comment announced. 3/31/14: Comments due.
Data Privacy	Department of Education	Guidance Issued	On 2/26/14, the Department of Education's Privacy Technical Assistance Center released guidance aimed to help school systems and teachers protect student privacy while using online educational services, like computer software, mobile applications and web-based programs provided by a third party to a school or school district. The guidance explains the Family Educational Rights and Privacy Act and the Protection of Pupil Rights Amendment. It also sets forth a list of suggested best practices, like remaining aware of which online educational services the district is currently using, maintaining awareness of other applicable laws, establishing policies and procedures to evaluate and approve new online educational services, and using a written contract or a legal agreement with providers.	2/26/14: Guidance issued.
Data Privacy Data Security Fair Credit Reporting Act ("FCRA")	FTC Equal Employment Opportunity Commission ("EEOC")	Guidance Issued	On 3/10/14, the FTC and EEOC jointly issued guidance on the proper use of background checks. The guidance explains how federal laws enforced by the FTC and EEOC apply to background checks performed for employment purposes. The guidance includes a document for employers and a separate document for employees explaining their rights under federal law when an employer or prospective employer conducts a background check.	3/10/14: Guidance issued.
Data Security	FTC	Motion to Transfer Venue Granted Motion to Dismiss Filed Stay Denied *FTC v. Wyndham Worldwide Corp.*, Case No. 2:12-cv-01365-SPL (D. Ariz. 3/25/13)	On 6/26/12, the FTC filed a complaint against Wyndham Worldwide Corp. in the U.S. District Court for the District of Arizona. The complaint was amended on 8/9/12. The FTC alleged that Wyndham and three of its subsidiaries violated Section 5 of the FTC Act by failing to take adequate security measures to protect personally identifiable information even after security breaches in 2008 and 2009. If the case goes to trial, it will be the first data privacy/security case fully litigated under Section 5. On 3/25/13, the U.S. District Court for the District of Arizona granted Wyndham's motion to transfer venue to the District of New Jersey. On 5/11/13, Wyndham filed a motion to dismiss arguing that the FTC lacks	6/26/12: Complaint filed. 8/9/12: Amended complaint filed. 3/25/13: Motion to transfer venue granted. 5/11/13: Motion to dismiss filed. 11/7/13: Stay

		FTC v. Wyndham Worldwide Corp., No 13-cv-01887 (D.N.J. 4/26/13)	jurisdiction to take such regulatory action. The FTC filed its response on 5/20/13. On 11/7/13, Judge Esther Salas of the U.S. District Court for the District of New Jersey denied Wyndham's motion for a stay of discovery pending Wyndham's motion to dismiss on the grounds that the FTC lacks authority to regulate data security. **See *FTC v. Wyndham Worldwide Corp.* in the "Courts" section for more information.**	denied.
Data Security	FTC	Administrative Complaint Filed Complaint Voluntarily Dismissed *LabMD, Inc. v. FTC*, No. 1:13-cv-01787 (D.D.C. complaint voluntarily dismissed 2/19/14) Complaint Refiled *LabMD, Inc. v. FTC*, No. 1:14-cv-00810-WSD (N.D. Ga. complaint filed 3/20/14)	On 8/28/13, the FTC filed a complaint against LabMD, Inc. alleging that LabMD exposed the personal information of nearly 10,000 consumers. The FTC's complaint alleges that LabMD failed to take reasonable and appropriate measures to prevent unauthorized disclosure of sensitive consumer data. On 11/12/13, LabMD filed a motion to dismiss the FTC's administrative complaint. On 11/14/13, LabMD filed a complaint in U.S. District Court against the FTC seeking declaratory and injunctive relief from the FTC's use of its unfairness authority to take enforcement action against LabMD's lax data security practices. LabMD alleges that the FTC engaged in "unconstitutional abuse of government power and ultra vires actions." LabMD also alleged that it is subject to HHS's regulatory jurisdiction, not the FTC's authority. LabMD became the second party, alongside Wyndham, to assert that the FTC's reading of its unfairness authority exceeds what Congress intended. On 1/16/14, the FTC denied LabMD's motion to dismiss the FTC's administrative enforcement action that gave rise to LabMD's filing a complaint against the FTC in U.S. District Court. On 2/19/14, LabMD dismissed its complaint against the FTC without prejudice. On 3/20/14, LabMD refiled its complaint challenging the FTC's authority to take enforcement action against the company for allegedly inadequate data security. LabMD had previously filed the complaint in the District for the District of Columbia but refiled the complaint in the Northern District of Georgia. Along with the complaint, LabMD filed a motion for preliminary injunction asking the court to enjoin the FTC from taking further enforcement action against it.	8/28/13: Complaint filed. 11/14/13: Complaint filed. 1/16/14: FTC denies LabMD's motion to dismiss administrative enforcement action. 2/19/14: Complaint Voluntarily Dismissed. 3/20/14: Complaint refiled.
Data Security	Federal Financial Institutions Examination Council	Final Guidance Released	On 1/23/13, FFIEC issued proposed guidance to financial institutions on the dangers of using social media in a less than secure online environment to attract customers. The proposed guidance discussed the applicability of consumer	1/23/13: Proposed guidance issued.

	("FFIEC")		protection and compliance laws, regulations, and policies to activities conducted via social media by banks, savings associations, and credit unions, as well as non-bank entities supervised by the Consumer Financial Protection Bureau ("CFPB") and state regulators. The proposed guidance was intended to help financial institutions identify potential risk areas and calls for establishing controls for an ongoing assessment of social media risk factors, and recommended implementing appropriate policies to identify, measure, monitor, and control the risks related to social media. Comments were due on 3/25/13. In their joint comments, the Center for Digital Democracy and U.S. PIRG Education Fund said that issuing guidance to financial institutions on social media is critically important. The groups asked FFIEC to go further and adopt new consumer privacy rules. On the other side of the debate, the Consumer Bankers Association ("CBA") told FFIEC it should rethink its proposed guidance. CBA stated that FFIEC's definition of social media is overbroad, and that a new risk management system was unnecessary. The National Association of Federal Credit Unions agreed with CBA, and stated that FFIEC's one-size-fits-all approach was inappropriate. On 12/11/13, FFIEC released final guidance on the dangers of using social media by banks, thrifts, and credit unions, as well as some non-bank entities supervised by the Consumer Financial Protection Bureau. The guidance states that the entities should consider using social media in the context of relevant consumer privacy laws and rules, like GLBA, FCRA, COPPA, CAN-SPAM and TCPA.	3/25/13: Comments filed. 12/11/13: Final guidance released.
Data Security Data Breach Internet of Things	FTC	Final Order Announced	On 9/4/13, the FTC reached a settlement with TRENDnet Inc. resolving allegations that TRENDnet failed to reasonably secure its Internet-connected cameras leading to the online posting of live feeds from those cameras. This is the first FTC enforcement action in the quickly developing space referred to as the "Internet of Things." The settlement terms require TRENDnet to refrain from misrepresenting the security of its devices, to notify its customers that its cameras had a flaw, and to obtain third-party assessments of TRENDnet's security programs every other year for the next 20 years. Comments on the proposed settlement were due on 10/4/13. On 2/10/14, the FTC issued a final order resolving the charges against TRENDnet.	9/4/13: Settlement reached. 10/4/13: Comments due. 2/10/14: Final order issued.

FEDERAL AGENCIES (continued)

Data Security Data Privacy	FTC	Proposed Consent Order Released Consent Order Adopted	On 10/22/13, the FTC released a proposed consent order with rent-to-own retailer Aaron's to settle claims of violations of Section 5 of the FTC Act. The complaint alleged that Aaron's surreptitiously monitored activities of its customers by logging keystrokes, capturing screenshots, and using the computer's webcam. The complaint further alleged that Aaron's tracked the physical location of rented computers. The consent order prohibits Aaron's from using monitoring technology and requires Aaron's to give clear notice and obtain express consent before installing technology that allows location tracking of a rented product. On 3/11/14, the FTC adopted the proposed consent order.	10/22/13: Consent order released. 3/11/14: Consent order adopted.
Data Security	FTC	Consent Order Approved *In re Accretive Health, Inc.*, File No. 122 3077 (Consent Order Announced 12/31/13)	On 12/31/13, the FTC proposed a consent order with a medical billing and revenue management services provider, Accretive Health, Inc. The FTC's complaint alleged that Accretive Health failed to employ reasonable and appropriate measures to protect personal information against unauthorized access. On 2/24/4, the FTC announced it approved the final consent order to resolve its complaint against Accretive Health.	12/31/13: Consent order proposed. 2/24/13: Final consent order approved.
Data Security	FTC	Consent Order Proposed *In re GMR Transcription Servs., Inc.*, File No. 122 3095 (Consent Order Proposed 1/31/14)	On 1/31/14, the FTC proposed a consent order with a medical transcription company, GMR Transcription Services, for failing to reasonably and appropriately secure consumers' personal information despite promises in its privacy policies that it would do so. The proposed settlement would prohibit GMR from misrepresenting the extent to which it protects consumers' personal information and would require GMR to implement a comprehensive information security program.	1/31/14: Consent order proposed.
Data Security	NIST	Report Released	On 2/18/14, NIST released a draft report asking for public comment on its role as an encryption standard-setting agency and in the standards-setting process. The report also asked for comment on the NSA's role as a stakeholder in the encryption standards process. Comments are due 4/18/14.	2/18/14: Report released. 4/18/14: Comments due.

FEDERAL AGENCIES (continued)

Data Security	NIST	Public Comment Sought	On 3/7/14, NIST published two draft documents seeking public comment on the processes for federal employees and contractors to use to securely access government computer resources through their mobile devices. The documents are titled "Guidelines for Derived Personal Identity Verification Credentials" and "Mobile, PIV, and Authentication." The federal government currently uses Personal Identification Verification smart cards and NIST is seeking to extend similar technology to mobile devices. Comments are due 4/21/14.	3/7/14: Public comment sought. 4/21/14: Comments due.
FCRA	FTC	Stipulated Final Judgment Announced *United States v. Infotrack Information Services, Inc.*, File No. 1:14-cv-02054 (N.D. Ill. stipulated final order 4/9/14) *United States v. Instant Checkmate, Inc.*, File No. 3:14-cv-00675-H-JMA (S.D. Cal. stipulated final order 4/9/14)	On 4/9/14, the FTC announced it reached stipulated final judgments with two defendants for violating the FCRA by providing reports about consumers to users such as prospective employers and landlords without taking reasonable steps to make sure they were accurate, or without making sure their users had a permissible reason to have the reports. The judgments impose a $525,000 fine against Instant Checkmate, Inc. and a $1 million fine against InfoTrack Information Services, Inc. All but $60,000 of the penalty against InfoTrack is suspended due to InfoTrack's inability to pay.	4/19/14: Final judgments announced.
Graham-Leach-Bliley Act ("GLBA")	Commodity Futures Trading Commission ("CFTC")	Best Practices Issued	On 2/26/14, the CFTC released best practices for financial institutions that must comply with GLBA Act provisions on data security and customer privacy. The guidance states that entities should: (i) have a written information security and privacy programs appropriate with the entity's size and complexity and scope of its activities; (ii) designate a senior-level employee with privacy and security management oversight responsibilities; (iii) identify in writing all reasonably foreseeable internal and external risks to the security and confidentiality of personal information and systems that process personal information and implement safeguards to control them; (iv) arrange for independent testing of the safeguards at least every two years; and (v) implement procedures for responding to incidents involving unauthorized access, disclosure, or use of personal information. Entities covered by the guidance include futures commission merchants, commodity	2/26/14: Best practices issued.

			trading advisers, commodity pool operators, introducing brokers, retail foreign exchange dealers, swap dealers, and major swap participants.	
GLBA	FTC	Notice of Intent to Request Public Comments Published	On 3/13/14, the FTC published a notice of intent to request public comments as the FTC plans to review its rules for safeguarding customer information under GLBA. The rules require pay day lenders, mortgage brokers, collection agencies, and other non-bank financial institutions to maintain a comprehensive data security program. These entities are also responsible for ensuring that their affiliates and service providers implement appropriate data safeguards.	3/13/14: Notice of intent to request public comments published.
Health Data Privacy and Security	Department of Health and Human Services ("HHS")	Final Omnibus HIPAA Rule Released Sample Business Associate Agreement Published HITECH Act Implementation Technical Corrections Issued Clarification Sought Model Notices of Privacy Practices Released	On 1/17/13, the Department of Health and Human Services ("HHS") issued the Final Omnibus Rule modifying the Privacy, Security, and Enforcement Rules promulgated under HIPAA as well as the Breach Notification Rule promulgated under the HITECH Act. Significant changes in the Final Omnibus Rule include: 1. Expanding the definition of "business associate" to include subcontractors and requiring business associates to enter into written contracts with their subcontractors that are substantially similar to business associate agreements; 2. Making business associates directly liable for compliance with all Security Rule standards and implementation specifications, as well as with certain Privacy Rule provisions; 3. Removing the limitations on liability of covered entities for the acts and omissions of business associates; 4. Revising the definition of marketing in the Privacy Rule to delineate which specific activities constitute marketing of PHI; 5. Requiring covered entities to obtain authorization from an individual for any disclosure of the individual's PHI in exchange for direct or indirect remunerations (*i.e.*, sale of PHI); 6. Increasing penalties for noncompliance with the HIPAA rules; 7. Granting individuals enhanced rights to receive electronic copies of	2/17/09: HITECH Act enacted. 4/17/09: HHS issued guidance on how to secure PHI and obtain exemption from breach notification. 8/25/09: HHS and FTC interim final regulations were published in the Federal Register. 2/22/10: Enforcement begun for breach notification provisions. 1/17/13: Final Omnibus HIPAA Rule released.

			their PHI and request restrictions on the disclosure of their PHI; 8. Requiring covered entities to change their privacy notices to describe certain uses and disclosures of PHI; 9. Modifying the Breach Notification Rule so that any acquisition, access, use, or disclosure of PHI not permitted under the Privacy Rule is presumed to be a breach unless a covered entity or business associate can demonstrate a low probability that the PHI has been compromised based on a four-factor assessment, and no longer using the significant risk of harm standard; and 10. Prohibiting health plans from using or disclosing genetic information for underwriting purposes, as required by the Genetic Information Nondiscrimination Act. The final rule became effective on 3/26/13, and covered entities and business associates were required to comply by 9/23/13. Existing business associate agreements are not required to comply until 9/23/14. On 1/25/13, HHS released sample business associate agreement provisions for use when revising contracts to comply with the Final Omnibus Rule. On 6/7/13, OCR published technical corrections to the Omnibus HIPAA Rule. Most of the corrections replace inaccurate references in the Final Omnibus Rule to sections of HIPAA. On 7/25/13, the Specialty Pharmacy Association of America ("SPAARx") asked HHS to clarify whether the Omnibus Rule prohibits pharmacies from using patient data without prior consent to conduct refill reminders and medication therapy management. On 9/13/13, HHS released its model notices of privacy practices to assist health care providers and health plans understand the ways in which they can notify patients of their privacy rights. The notices can be provided in a booklet, a layered notice, a full-page presentation, or as a text-only version.	1/25/13: Sample business associate agreement released. 3/26/13: Effective date of Final Omnibus HIPAA Rule. 6/7/13: Technical corrections issued. 7/25/13: Clarification sought. 9/13/13: Model notices of privacy practices released. 9/23/13: Effective date of Final HIPAA Omnibus Rule on covered entities and business associates. 9/23/14: Deadline to comply for existing business associate agreements.
Health Data Privacy and Security	HHS	Comment Sought New Policy Announced	On 8/6/13, HHS's CMS posted a request for comment on the most appropriate policy for the agency to follow when releasing Medicare physician payment data. The request for comment follows the U.S. District Court for the Middle District of Florida's lifting an injunction, in place since 1979, that prohibited HHS from releasing Medicare physician reimbursement data that would identify specific physicians. The deadline to submit comments was 9/5/13.	8/6/13: Comments sought. 9/5/13: Comments due. 1/14/14: New

			On 1/14/14, CMS instituted a new policy for releasing data on the amounts of Medicare payment to doctors under FOIA that will rely on an individualized approach to requests. CMS said it will take a case-by-case determination. CMS said that this policy change will be a step forward in making Medicare data more transparent and accessible. On 4/2/14, CMS stated that it planned to release Medicare payment data through its website. On 4/9/14, the Washington Post, Wall Street Journal, and several other news organizations ran stories after analyzing the Medicare payment data.	policy released. 4/2/14: Data to be released through CMS website. 4/9/14: Articles published.
Health Data Privacy and Security	HHS	Notice Published Second Notice Published	On 10/23/13, CMS published a notice modifying the Health Insurance Exchanges Program system of records that collects personal information about individuals who apply for enrollment or exemptions in a qualified health plan. CMS's notice proposed several small modifications, such as: (i) clarifying that federal tax return information may be disclosed; (ii) adding a description of the information resulting from registering, training, and certifying individuals who will assist consumers in states where a federal exchange operates, and (iii) clarifying that information may be disclosed to states where the ACA enrollment assisters will be operating, and that information on agents and brokers may be displayed on the federal websites. On 12/2/13, CMS published another notice modifying the Health Insurance Exchanges Program system to make it easier for state exchanges to disclose personally identifiable information collected from health insurance applicants. The proposed modification would allow an exchange to use or disclose eligibility and enrollment PII to ensure the efficient operation of an Exchange through the uses or disclosures that may not be directly connected to minimum functions. The modification would also give the HHS Secretary the ability to approve other types of PII disclosures if the information would be used only for the purpose of ensuring efficient operation of an exchange.	10/23/13: Notice published. 11/22:13: Modification went into effect. 12/2/13: Notice published.
Health Data Privacy and Security	HHS	Report Released	On 12/4/13, HHS's inspector general released a report raising concerns about how well HHS's Office of Civil Rights is carrying out its oversight of compliance with securing ePHI under the HIPAA Security Rule. The report stated that OCR had not met requirements under the HITECH Act that it conduct periodic audits of covered entities to ensure compliance with the Security Rule. OCR responded to the audit in formal comments by stating that it developed an audit protocol and implemented a pilot audit program in 2012. However, OCR stated it has not implemented a permanent audit program because no federal	12/4/13: Report released.

			funding has been appropriated for the program.	
Health Data Privacy and Security	HHS	Report Released	On 12/10/13, HHS's inspector general released a report stating that hospitals with electronic health records ("EHRs") may not be doing enough to prevent fraud related to the technology. The report stated that nearly all of the 864 hospitals that received federal incentive payments for adopting EHRs had in place the recommended audit functions and safeguards for protecting health data. However, the report found that the hospitals may not be using those audit functions and safeguards to their full capability.	12/10/13: Report released.
Health Data Privacy and Security	HHS	Settlement Announced	On 12/26/13, HHS announced it reached a $150,000 settlement with a Massachusetts-based dermatology practice, Adult & Pediatric Dermatology PC, for violating HIPAA for failing to have sufficient policies and procedures in place to address the breach notification provisions of the HITECH Act.	12/26/13: Settlement announced.
Health Data Privacy and Security	HHS DOJ	Proposed Rules Published	On 1/7/14, HHS published a proposed rule stating that the rule would remove unnecessary legal barriers from health privacy rules that may prevent states from reporting certain information about people who are banned from buying guns for mental health reasons. The rule change affects the HIPAA Privacy Rule and reporting to the National Instant Criminal Background Check System ("NICS"). The modification would permit certain HIPAA-covered entities to disclose to NICS the identities of persons prohibited by federal law from possessing or receiving a firearm for reasons related to mental health. Comments were due 3/10/14. Separately, on 1/7/14, DOJ published a proposed regulation that would clarify who, due to mental health reasons, is prohibited under federal law from receiving, possessing, shipping, or transporting firearms. DOJ's proposed regulation would clarify the definition of terms "adjudicated as a mental defective" and "committed to a mental institution." Comments were due 4/7/14.	1/7/14: HHS and DOJ proposed rules published. 3/10/14: HHS proposed rule comments due. 4/7/14: DOJ proposed rule comments due.
Health Data Privacy and Security	HHS	Guidance Issued	On 2/21/14, HHS's OCR issued guidance on how the HIPAA Privacy Rule applies to mental health records. The guidance clarifies when health care providers are permitted under the Privacy Rule to release a patient's mental health records to family members and others, including law enforcement. The guidance states that when a patient is present and has the capacity to make health care decisions, health care providers may communicate with a patient's family, friends, or other persons the patient has involved in his or her health care or payment for care, so long as the patient does not object. Where a patient isn't present or is incapacitated, health care providers may share mental health data with family, friends, and others as long as the health care provider determines that	2/21/14: Guidance issued.

			doing so is in the best interests of the patient.	
Health Data Privacy and Security	HHS	Settlement Announced	On 3/7/14, HHS announced its first HIPAA settlement with a county government. HHS and Skagit County, Washington reached an agreement whereby Skagit County agreed to pay $215,000 to settle allegations that Skagit County's public health department violated HIPAA when patients' data were exposed electronically.	3/7/14: Settlement announced.
Health Data Privacy and Security	HHS	Guidance Released	On 3/28/14, HHS released a security risk assessment tool to guide providers in small- and medium-sized practices in assessing their data security safeguards. The tool is meant to walk providers through all aspects of an information security risk assessment and prompt documentation of the assessment. The tool can also produce a post-assessment report that providers can give to auditors. It is available as a downloadable application.	3/28/14: Guidance released.
Telemarketing	FTC	Stipulated Final Judgment Announced *FTC v. ELH Consulting, LLC*, Case No. 2:12-cv-02246 (D. Ariz. Stipulated final judgment entered 10/16/13) *FTC v. Purchase Power Solutions LLC* *FTC v. Allied Corporate Connection LLC* *FTC v. Complete Financial Strategies LLC* *FTC v. Holley* *FTC v. Miller*	On 11/22/13, the FTC announced it entered into stipulated final judgments with six robocallers allegedly participating in a scheme to make unlawful robocalls from "Rachel." As part of the judgment, the six defendants agree to pay $11.9 million to settle the claims of deceptive credit card interest rate reduction scams and violating the Telemarketing Sales Rule.	11/22/13: Stipulated final judgment announced.
Telemarketing	FTC	Report Issued	On 12/23/13, the FTC released its biennial report to Congress under the Do Not Call Registry Fee Extension Act of 2007. The FTC's report details an increase in	12/23/13: Report

			the number of registrations on the national Do Not Call Registry. The FTC stated that 5.8 million registrations were added in the 2013 fiscal year, to a total of 223 million registrations.	issued.
Telemarketing	FTC	Stipulated Final Judgments Announced *FTC v. SubscriberBASE Holdings, Inc.*, Case No. 1:13-cv-01527 (N.D. Ill. stipulated final judgments released 2/19/14)	On 2/18/14, the FTC announced it reached stipulated final judgments with twelve defendants who hired affiliate marketers to send millions of spam text messages. The defendants agreed to pay $2.5 million to resolve allegations that they deceived consumers and resold consumers' personal information to third parties with their "free $1,000 gift card" text messages.	2/18/14: Stipulated final judgments announced.
Telemarketing	FTC	Stipulated Final Judgment Announced *FTC v. CPATank, Inc.*, Case No. 1:14-cv-01239 (N.D. Ill. stipulated final judgment 2/25/14)	On 2/28/14, the FTC announced it entered a stipulated final judgment with a group of affiliate marketers it accused of sending unlawful spam in an alleged "free" gift card scam. The FTC's complaint alleged that CPATank sent illegal text messages through a third party. The stipulated final judgment assesses a $200,000 judgment and prohibits CPATank from making or initiating further spam.	2/28/14: Stipulated final judgment announced.
Telemarketing	FTC	Stipulated Final Judgment Announced *United States v. Versatile Marketing Solutions, Inc.*, Case No. 1:14-cv-10612-PBS (D. Mass. proposed stipulated final order filed 3/10/14)	On 3/12/14, the FTC announced it entered into a stipulated final judgment with a home security company, Versatile Marketing Solutions Inc., that made millions of phone calls to consumers on the FTC's Do Not Call Registry. The complaint alleged violations of the FTC's Telemarketing Sales Rule. The stipulated final judgment includes a $3.4 million judgment, with all but $320,700 suspended due to inability to pay, and prohibits Versatile Marketing Solutions from making abusive telemarketing calls and from calling any consumer on the Do Not Call Registry.	3/12/14: Stipulated final judgment announced.

STATES				
Topic / Key Words	**State**	**Bill / Law**	**Description**	**Status / Comments**
Children's Privacy	California	S.B. 568 Sponsor: Steinberg	This legislation would require operators of websites, social media sites and mobile apps, at the request of a minor child who is a registered user of the site, to delete information previously posted by the minor. The requirement would take effect by January 2015 and would require operators to provide notice that minors can remove content.	2/22/13: Introduced and subsequently referred to the Judiciary Committee. 4/23/13: Approved by the Judiciary Committee. 4/29/13: Passed Senate; received in the Assembly and subsequently referred to several committees. 8/26/13: Passed Assembly. 9/23/13: Signed by Governor. 1/1/15: Effective date.
Children's Privacy	Maryland	Workgroup Report	The Maryland Attorney General submitted a Workgroup on Children's Online Privacy Protection final report to state lawmakers. The report provides information on digital privacy issues pertaining to children and is intended to guide legislative committees working on the topic. The recommendations for legislation include requiring that sensitive information about children be encrypted and adopting data minimization rules similar to those of the EU for information collected from and/or about teens and children.	12/30/13: Report submitted.
Children's Privacy	California	S.B. 1177 Sponsor: Steinberg	This bill would prohibit websites, online services, and Web and mobile applications used for grades K-12 from marketing or advertising to student users, and from compiling or sharing the personal information of students beyond what is necessary. It also requires these services to delete information that is no longer needed for its original purpose.	2/20/14: Introduced and referred to Committee on Rules.
Children's Privacy	South Carolina	S. 148	The bill would allow parents and guardians to place a freeze on credit reports for "protected customers," defined as persons	1/8/13: Introduced in Senate.

STATES (continued)				
Privacy of Persons with Special Needs		Sponsors: Shealy, Bryant, Gregory, Alexander	under the age of 16, or incapacitated persons or protected persons for whom a guardian or conservator has been appointed. Consumer reporting agencies would be prohibited from charging parents or guardians a fee to place this freeze.	4/25/13: Passed Senate. 3/5/14: Passed House. 4/7/14: Signed by Governor. 1/1/15: Effective date.
Consumer Privacy, General	California	S.B. 383 Sponsor: Jackson	The measure would amend the Song-Beverly Credit Card Act, tightening consumer privacy in credit card transactions. It would authorize a person or entity that accepts credit cards in an online transaction involving an electronic downloadable product to require a cardholder to provide the billing zip code and street address number associated with the card.	2/20/13: Introduced and referred to Rules Committee. 1/30/14: Passed Senate.
Consumer Privacy, General	California	S.B. 1351 Sponsor: Hill	The measure would require payment card companies to issue only credit and debit cards that include an embedded microchip containing personal data and would require customers to input a personal identification number at the point of sale to complete a transaction. It would also require that retailers put in place card readers that accept either a magnetic stripe swipe or a chip and PIN transaction.	2/21/14: Introduced in Senate.
Consumer Online Privacy	Various		Google agreed to a $17 million settlement with 37 states and the District of Columbia over allegations that it overrode the privacy settings of Apple Inc.'s Safari web browser to track users without their knowledge. New York and Maryland headed the settlement efforts and will each receive about $1 million in civil penalty payments.	11/12/13: Settlement reached.
Consumer Online Privacy	New Jersey	Administrative Action	A Tennessee-based data aggregation and analytics company has agreed to pay $400,000 to settle New Jersey administrative enforcement action claims that the company engaged in "history sniffing," or use of JavaScript code to scan the browsing history of consumers, without their knowledge or consent.	11/15/13: Settlement reached.
Data Breach	California	Health Care Providers Guidance	The guidance makes recommendations to health care providers, including that they raise awareness within their organizations of medical identity theft as a quality-of-care issue and that they implement preventative measures such as anomaly detection and data flagging. It advises health insurers to use fraud-detection	10/17/13: Report released.

STATES (continued)

			software to flag claims that could be the result of identity theft. It also incorporates guidance form the FTC, which notes that giving victims of identity theft copies of their own health records is not a violation of the identity thief's HIPAA rights.	
Data Breach	Attorneys General of Connecticut and Illinois	Investigation	The attorneys general of Connecticut and Illinois are leading an investigation, together with attorneys general from approximately 30 other states, into the recent data breaches at Target and Neiman Marcus detailed in the Industry Section.	1/15/14: Press release announcing leadership of investigation.
Data Breach	Kentucky	H.B. 5 Sponsor: Butler	The bill would require public agencies to safeguard personal information and notify affected individuals if their information is breached by the state. It would also require the state Department for Libraries and Archives to establish "procedures to protect against unauthorized access to personal information" as well as data disposal and destruction procedures. State legislative and judicial branches would also be covered by the bill.	1/9/14: Introduced in House. 1/23/14: Approved by the House State Government Committee. 3/21/14: Passed Senate. 3/28/14: Passed House. 4/10/14: Signed by Governor. 1/1/15: Effective date.
Data Breach	Kentucky	H.B. 232 Sponsors: Riggs, King, Westrom	The bill would require companies to notify affected individuals of unauthorized access to their personal information if there is actual identity theft or fraud or if the company reasonably believes the breach has caused or will cause identity theft or fraud. If the breach involves 1,000 or more Kentucky residents, the bill also requires the company to notify the major credit reporting agencies of the breach. The bill also contains a provision prohibiting a cloud computing service provider from using or facilitating the use of student data for advertising purposes and from selling student data for commercial purposes.	1/21/14: Introduced in House. 3/10/14: Passed House. 3/31/14: Passed Senate. 4/10/14: Signed by Governor. 1/1/15: Effective date.
Data Breach	New Mexico	H.B. 224 Sponsor: Rehm	The bill would require covered entities to notify affected individuals of a breach of their unencrypted personal information within 10 days of discovering the breach, and also to notify the state attorney general if more than 50 New Mexico residents must be notified. The bill would also impose data disposal and data security requirements on companies	1/29/14: Introduced in House. 2/20/14: Legislature adjourned for the year without completing action on the bill.

STATES (continued)

			operating in New Mexico. The bill authorizes the state attorney general to seek injunctive relief and actual damages related to a breach, and also provides for a private right of action.	
Data Breach	Minnesota	H.F. 2253 Sponsor: Schoen	The bill would amend Minnesota's data breach notification statute to require all covered entities that experience a breach to notify affected individuals within 48 hours of discovering the breach, and also to provide one year of free credit monitoring services to affected individuals.	2/25/14: Introduced in House.
Data Breach	California	Cybersecurity Guidance	Attorney General Harris released a guide primarily targeted toward small businesses, "Cybersecurity in the Golden State," advising on measures to improve cybersecurity, such as educating workers about security data, updating and employing security software, encrypting data and using effective passwords, and creating a disaster plan.	2/27/14: Guidance released.
Data Breach	Texas	S.B. 1610 Sponsor: Schwertner	S.B. 1610 amends the state's data breach law to provide that, in the event of a computer security breach involving personal information of a person who does not reside in Texas, the required notice to that individual may be provided under either Texas law or the law of the state in which the person resides.	3/8/13: Introduced and subsequently referred to committee. 4/25/13: Passed Senate. 5/22/13: Passed House. 6/14/13: Signed by Governor and took effect immediately.
Data Breach	Iowa	S.F. 2259	The bill would amend Iowa's data breach law to require covered entities to notify the state attorney general of breaches affecting more than 500 Iowans. The attorney general notification must occur within five business days after notifying affected individuals.	2/20/14: Introduced in Senate. 2/26/14: Passed Senate. 3/18/14: Passed House. 4/3/14: Signed by Governor. 7/1/14: Effective date.
Do Not Track	California	A.B. 370 Sponsor: Muratsuchi	The bill would require an operator of a commercial website or online service that collects personally identifiable information through the Internet about consumers residing in California to disclose how it complies with a user's request to disable online tracking. The California Attorney General is expected to issue guidance	2/14/13: Introduced and subsequently referred to several committees. 5/2/13: Passed Assembly and received in the Senate.

STATES (continued)

			regarding best practices for compliance with this law in the coming months.	8/22/13: Passed Senate. 9/27/13: Signed by Governor. 1/1/14: Effective date.
Email Privacy	California	S.B. 467 Sponsor: Leno	This bill would prohibit a governmental entity, as defined, from obtaining the contents of a wire or electronic communication from a provider of electronic communication services or remote computing services that is stored, held, or maintained by that service provider, without a valid search warrant. It was vetoed in October by Governor Jerry Brown, who said the bill would impede ongoing criminal investigations.	2/21/13: Introduced and referred to committee. 5/14/13: Passed Senate. 8/22/13: Passed Assembly. 9/18/13: Presented to Governor for signature. 10/12/13: Vetoed by Governor.
Email Privacy	Texas	H.B. 2268 Sponsor: Carona	The bill would require a state law enforcement agency to obtain a warrant prior to accessing electronic customer data held in electronic storage, including emails, regardless of the age of the electronic documents. The bill would apply with respect to a business or other entity doing business in Texas under a contract or a terms of service agreement with a resident of Texas if any part of the contract or agreement is to be performed in Texas.	3/4/13: Introduced and subsequently referred to the Committee on Criminal Jurisprudence. 5/7/13: Passed House. 5/22/13: Passed Senate, as amended. 5/24/13: House concurred in Senate amendments. 6/14/13: Signed by Governor and took effect immediately.
Social Media	Various	Restrictions on employer access to social media user names and/or passwords	Legislation to regulate employer access to personal social media accounts is pending in a number of states, including California (A.B. 25), Florida (H.B. 527; S.B. 198), Georgia (H.B. 117; H.B. 149), Hawaii (H.B. 713), Massachusetts (S.B. 852), Minnesota (H.F. 293), Missouri (H.B. 1834), Nebraska (L.B. 58), New York (A. 443; S. 1701), North Carolina (H.B. 846), and Oklahoma (H.B. 2372). The measures enacted into law thus far are described below.	

STATES (continued)				
Social Media	Arkansas	H.B. 1901/Act 1480 Sponsor: Steel	The measure prohibits an employer from requiring or requesting a current or prospective employee to disclose social media account access information or content.	3/8/13: Introduced and referred to the Committee on Public Health, Welfare and Labor. 3/28/13: Passed House. 4/16/13: Passed Senate. 4/22/13: Signed by Governor as Act 1480. 8/15/13: Effective date.
Social Media	Colorado	H.B. 1046 Sponsor: Williams	Under the bill, an employer is prohibited from suggesting, requesting, or requiring an employee or applicant to disclose any user name, password, or other means for accessing the employee's or applicant's personal account or service through the employee's or applicant's personal electronic communications device, and is also prohibited from compelling an employee or applicant to add anyone, including the employer, to the employee's or applicant's social media contacts.	1/9/13: Introduced and referred to the House Business, Labor, Economic, and Workforce Development Committee. 3/5/13: Passed House. 4/19/13: Passed Senate. 5/11/13: Signed by Governor and took effect immediately.
Social Media	Illinois	S.B. 2306 Sponsor: Radogno	This legislation amends the state's existing Right to Privacy in the Workplace Act to provide that the Act's restriction on an employer's request for information concerning an employee's social networking profile or website applies only to the employee's personal account.	2/15/13: Introduced and referred to committee. 4/23/13: Passed Senate. 5/21/13: Passed House. 8/16/13: Signed by Governor. 1/1/14: Effective date.
Social Media	Nevada	A.B. 181 Sponsors: Multiple	The legislation prohibits an employer from conditioning the employment of an employee or prospective employee on his or her disclosure of the user name, password or any other information that provides access to the employee's or prospective employee's personal social media account.	3/1/13: Introduced and referred to Committee on Commerce and Labor. 3/26/13: Passed Assembly. 5/21/13: Passed Senate. 6/13/13: Signed by Governor.

STATES (continued)

				10/1/13: Effective date.
Social Media	New Mexico	S.B. 371 Sponsor: Candelaria	The legislation prohibits an employer from requesting or demanding a prospective employee's social networking password or otherwise mandating access to the account. The prohibition does not cover current employees.	1/31/13: Introduced and referred to Senate Public Affairs Committee and Senate Judiciary Committee. 3/1/13: Passed Senate. 3/16/13: Passed House. 4/5/13: Signed by Governor. 6/14/13: Effective date.
Social Media	New Jersey	A. 2878 Sponsor: Burzichelli	This bill would prohibit an employer from requiring disclosure of a current or prospective employee's user name, password, or other means for accessing a social networking account or service.	5/10/12: Introduced and referred to Assembly Consumer Affairs Committee. 6/25/12: Passed Assembly. 10/25/12: Passed Senate. 3/21/13: Passed in final form by both houses. 5/6/13: Conditionally vetoed by Governor, with recommendations for amendment. 5/20/13: Passed again by both houses after concurrence with Governor's recommendations. 8/28/13: Signed by Governor. 12/1/13: Effective date.
Social Media	Oregon	H.B. 2654 Sponsor: Doherty	This measure prohibits an employer from compelling an employee or applicant for employment to provide access to a personal social media account or to add the employer to the employee's social media contact list, and prohibits retaliation by an employer against an employee or applicant for refusal to provide access to accounts or to add the employer to the	1/14/13: Introduced and subsequently referred to committee. 4/15/13: Passed House.

STATES (continued)

			contact list.	5/14/13: Passed Senate. 5/22/13: Signed by Governor. 1/1/14: Effective date.
Social Media	Utah	H.B. 100 Sponsor: Barlow	This legislation prohibits an employer from requesting an employee or applicant for employment to disclose a social media password or to take adverse action, fail to hire, or otherwise penalize an employee or applicant for failing to disclose such information.	2/1/13: Introduced and referred to House Public Utilities and Technology Committee. 2/21/13: Passed House. 3/5/13: Passed Senate. 3/26/13: Signed by Governor. 5/14/13: Effective date.
Social Media	Washington	S.B. 5211 Sponsor: Hobbs	This measure prohibits an employer from requesting, requiring, or otherwise coercing an employee or applicant to disclose login information for the employee or applicant's personal social networking account.	1/23/13: Introduced and referred to Senate Commerce and Labor Committee. 3/13/13: Passed Senate. 4/17/13: Passed House. 5/21/13: Signed by Governor. 7/28/13: Effective date.
Social Media	Wisconsin	S.B. 223 Sponsor: Sargent	This measure prohibits employers, educational institutions, and landlords from demanding access to social media information from employees, job applicants, tenants, prospective tenants, and students. It also prevents employers, educational institutions, and landlords from penalizing individuals who exercise their rights under the proposed law.	6/27/13: Introduced and referred to Committee on Judiciary and Labor. 11/12/13: Passed Senate. 1/21/14: Passed Assembly. 4/8/14: Signed by Governor. 4/10/14: Effective date.

COURTS				
Topic / Key Words	**Name**	**Action**	**Description**	**Status / Comments**
California Anti-Spam Law Maryland Anti-Spam Law	*Beyond Systems Inc v. Kraft Foods Inc.*, 13-2137 (4th Cir. 2/25/14)	Motion for Summary Judgment Granted Appeal Filed	The Fourth Circuit is considering a case that could significantly impact plaintiffs' ability to establish standing under California's and Maryland's anti-spam laws. The suit arose in 2008 when Beyond Systems Inc ("BSI")sued Kraft claiming it received 600,000 spam emails from Kraft through another company, Connexus. Both California and Maryland allow Internet service providers ("ISPs") to sue suspected spamming companies, and BSI claimed standing because it met the *de minimis* requirements under the respective definitions of both statutes to qualify as an ISP even though it could not demonstrate that it was a "bona fide" ISP. On 8/12/13, a Maryland district court judge granted Kraft's motion for summary judgment, holding that BSI lacked standing because it was not a bona fide ISP. The court explained allowing a non-bona fide ISP to have standing would create the situation Congress sought to avoid when it added the preemption exception in the CAN-SPAM Act. On 9/16/13, BSI filed a notice of appeal. The case has been fully briefed, but no oral argument has been scheduled.	8/12/13: Motion for summary judgment granted. 9/16/13: Notice of appeal filed.
California Invasion of Privacy Act	*Young v. Hilton Worldwide Inc.*, No. 12-56189 (9th Cir. 3/20/14) *Young v. Hilton Worldwide Inc.*, No. 12-56189 (C.D. Cal. 6/18/12)	Dismissal Reversed	On 3/20/14, the Ninth Circuit reversed the dismissal of a class action for violations of the eavesdropping provisions of California's Invasion of Privacy Act. The plaintiffs had alleged that Hilton recorded phone calls to a customer service line over which financial information was exchanged without the plaintiffs' consent. The complaint contained two counts, one for eavesdropping and recording on a land line and the other for the eavesdropping and recordation on a cellular or cordless telephone line. The district court dismissed the case on the ground that the plaintiff did not allege that the calls were confidential. The Ninth Circuit held that plaintiffs were not required to allege confidentiality with respect to cell phone calls under California Supreme Court precedent, even though this requirement exists for landline telephone calls.	3/20/14: Dismissal reversed and case remanded to the lower court.
California "Shine the Light" Statute	*Baxter v. Rodale*, No. 12-56925 (9th Cir. 2/21/14) *Boorstein v. CBS Interactive Inc.*, No. B24742 (Cal. App.	Complaints Filed Motions to Dismiss Filed Notices of Appeal Filed	Class action lawsuits were filed in late 2011 and early 2012 against website operators, especially magazine publishers, in California state and federal courts alleging violations of California's "Shine the Light" law, which applies to the sharing of personal information collected online or offline with third parties for the third parties' own marketing purposes. The statute requires businesses that collect and share personal information to disclose to consumers upon request what information is shared and with whom. In the	Dec. 2011 – Jan. 2012: Complaints filed. Aug. 2012 – Nov. 2012: Cases dismissed (*Rodale*, *Men's Journal*, *Time*, *Condé Nast*, *Hearst*).

	Ct. 3/12/14) *Boorstein v. Men's Journal LLC*, No. 12-56696 (9th Cir. 2/21/14) *Golba v. Reader's Digest Ass'n*, No. 8:12-cv-00361-DOC-MLG (C.D. Cal. 3/8/12) *King v. Condé Nast Pubs.*, No. 12-57209 (9th Cir. 2/18/14) *Miller v. Hearst Commc'ns*, No. 12-57231 (9th Cir. 2/18/14) *Murray v. Time Inc.*, No. 12-17591 (9th Cir. 2/18/14)	Opinion Issued (*Condé Nast*) Opinion Issued (*Hearst*) Opinion Issued (*Time*) Opinion Issued (*Rodale*) Motion to Dismiss Granted (*Men's Journal*) Opinion Issued (*CBS Interactive*)	alternative, businesses may provide consumers the ability to opt out of sharing. The complaints allege problems ranging from failures to properly label website links to failures to contain specific text in privacy policies. Under the plaintiffs' view of the law, defendants must include the text "Your Privacy Rights" on their home page, linking to a page entitled "Your Privacy Rights." Plaintiffs assert defendants must also designate contact information for customers to deliver their Shine the Light requests. Finally, plaintiffs assert that defendants must clearly describe California customers' rights under the law. The complaints also allege violations of the California Unfair Competition Law, which prohibits unfair business practices. Motions to dismiss have been filed and granted in several of the cases. Defendants have successfully argued that plaintiffs have not exercised their rights by making requests under the law, that defendants have not failed to respond, and that, in any event, plaintiffs have not been injured and thus have no standing. Plaintiffs have generally filed amended complaints, which have again been dismissed or are pending. Multiple appeals have been filed following the dismissals at the trial court level. On 12/4/12, the court in *Golba* issued a stay pending resolution of the other appeals. On 12/19/13, the Ninth Circuit in *CBS Interactive* affirmed the lower court's dismissal of the case for lack of standing. The California Supreme Court refused review of the *CBS Interactive* case on 3/12/14. In February, the Ninth Circuit similarly dismissed all other pending appeals for lack of standing based on plaintiffs' failure to submit an information request.	12/4/12: Case stayed (*Golba*). 12/31/12: Demurrer sustained; case dismissed (*CBS Interactive*). 3/13/13: Notice of appeal filed (*CBS Interactive*). 3/27/13: Appeals consolidated (*Rodale*, *Men's Journal*, *Time*, *Condé Nast*, *Hearst*). 12/19/13: Opinion issued (*CBS Interactive*). 2/18/14: Opinion issued (*Condé Nast*, *Hearst*, *Time*) 2/21/14: Opinion issued (*Rodale*); joint motion to dismiss granted (*Men's Journal*). 3/12/14: Petition for review denied by CA Supreme Court (*CBS Interactive*).
California Song-Beverly Credit Card Act	*Mehrens v. Redbox Automated Retail LLC*, No. 12-55234 (9th Cir. 1/8/14) *Apple Inc. v. S.C. (Krescent)*, No. S199384 (Cal. 2/4/13)	Motion to Dismiss Granted (*Mehrens*) Opinion Issued (*Apple*) Appellate Briefs Filed (*Mehrens*)	The California Song-Beverly Credit Card Act prohibits in-person collection of personal information that is not necessary to complete a credit card transaction. The goal of the legislation was to prevent merchants from asking for this information for the purpose of fraud prevention, but then later using it for marketing. In *Mehrens*, the district court granted the defendant's motion to dismiss, holding the Act inapplicable in the context of online transactions and transactions at stand-alone kiosks. On 2/4/13, the California Supreme Court in *Apple* reversed a lower court and held that the law does not apply to online transactions. The court reasoned that the prohibition on collection of personal information does not apply to online retailers that do not have the same opportunity to take the same anti-fraud steps as brick-and-mortar retailers, e.g. comparing a consumer's signature on a receipt to the signature on the consumer's credit card or examining	3/14/12: Petition for review granted (*Apple*). 8/1/12: Joint motion to stay granted (*Mehrens*). 11/7/12: Oral arguments heard (*Apple*). 2/4/13: Opinion issued (*Apple*). 4/15/13: Opening brief filed (*Mehrens*).

			photo identification. The *Mehrens* appeal had been stayed pending the California Supreme Court's decision; on 3/12/13, the court permitted the appellant to file a replacement opening brief in light of the decision in *Apple*. Briefs have been filed; oral argument was held on 1/8/14 but no opinion has been issued.	6/17/13: Opposition brief filed (*Mehrens*). 6/28/13: Reply brief filed (*Mehrens*). 1/8/14: Oral argument held (*Mehrens*).
Class Action Fairness Act ("CAFA")	*Wood v. Lowe's Home Center Inc.*, No. 13-cv-00584 (E.D. Mo. 7/30/13) *Watson v. Kohl's Dep't Stores Inc.*, No. 13-cv-00600 (E.D. Mo. 4/16/13) *Tyler v. Gap Inc.*, No. 13-cv-00581 (E.D. Mo. 1/14/14)	Complaints Filed Case Remanded (*Watson*) Motions to Remand Filed (*Wood; Tyler*) Motion to Remand Granted (*Wood*) Motion to Dismiss Granted (*Tyler*)	A series of proposed class action complaints filed by the same law firm in Missouri alleges that major retailers operating in the state, including Lowe's, Kohl's, and Old Navy, are liable for invading consumers' privacy by installing cookies and other tracking technologies on the computers of users who visit the retailers' websites. In the view of the defendants, potential damages in the cases range from $19 million against Old Navy to over $600 million against Kohl's. The plaintiffs, however, have attempted to defeat federal jurisdiction by stipulating that total class damages would not exceed the CAFA threshold of $5 million. The retailers removed all three cases to federal court, and plaintiffs have moved to remand. On 4/16/13, the court in *Watson* granted the motion to remand, finding that the proffered stipulation was irrelevant in light of the U.S. Supreme Court's recent decision in *Knowles* (see above), but also that Kohl's had not produced any evidence to show that damages would exceed the threshold. The Eighth Circuit refused to hear an interlocutory appeal. On 7/30/13, the court in *Wood* followed suit, holding that Lowe's could not avoid remand by citing the result of discovery in other cases showing that damages would likely exceed the CAFA threshold. On 1/14/14, the court in *Tyler* granted the parties' joint motion to dismiss the case with prejudice.	4/16/13: Case remanded to state court (*Watson*). 4/19/13: Motion to remand (*Wood*). 4/25/13: Motion to remand (*Tyler*). 7/30/13: Case remanded to state court (*Wood*). 1/14/14: Joint Motion to dismiss granted (*Tyler*).
Computer Fraud and Abuse Act ("CFAA")	*In re Google Android Consumer Privacy Litig.*, No. 3:11-md-02264 (N.D. Cal. 3/12/14)	Motion to Dismiss Partially Granted	On 3/12/14, a federal judge partially granted Google's motion to dismiss claims that Google had collected and shared user information through apps on its Android mobile platform without consent. The court dismissed plaintiff's CFAA claims because plaintiffs failed to show that Google's conduct impaired their mobile devices or interrupted their mobile service so as to cause damage or loss in excess of $5,000. The court allowed plaintiff's claims under California's Unfair Competition Law to proceed.	3/12/14: Motion to dismiss partially granted.
Computer Fraud and Abuse Act ("CFAA")	*United States v. Nosal*, No. 10-10038 (9th Cir.	Opinion Issued Motion to Dismiss	The Ninth Circuit agreed to rehear *en banc* a case that allowed a criminal prosecution under the CFAA of a defendant accused of accessing data stored on his employer's corporate network in violation of prominently displayed warnings about restrictions on its use and the disclosure of	10/27/11: Rehearing granted. 4/10/12: *En banc* opinion

	8/3/12) *United States v. Nosal*, No. CR-08-0237 (N.D. Cal. 1/8/14) *United States v. Nosal*, No.14-10037 (9th Cir. 1/27/14)	Denied Defendant Convicted	information stored there. On 4/10/12, the court reversed the panel decision and affirmed the district court's holding, explaining that the CFAA was meant to target hackers and does not criminalize violations of computer or website computer use restrictions. The court strongly disputed the government's broad interpretation of the CFAA, observing that it would make every violation of a private computer use policy (including, perhaps, playing games or shopping online) into a federal crime. The court noted that this decision put it at odds with decisions in the Fifth, Seventh, and Eleventh Circuits that interpreted the CFAA more broadly. The judgment was stayed 120 days pending a possible appeal to the Supreme Court; the government opted against the appeal, and the mandate issued 8/3/12. On remand, the district court considered the Ninth Circuit's opinion but refused to dismiss the remaining CFAA-related claims, which involve wholly unauthorized access of data by the defendant after he had left his employer. In denying the defendant's motion, the court rejected his argument that the Ninth Circuit's opinion added an element to CFAA violations that would require the prosecution to show that the defendant "circumvent[ed] technological access barriers" to access the information. The defendant was ultimately convicted on the CFAA counts and motions to overturn the verdict were denied. On 1/8/14, defendant was sentenced to a year-long prison term and community service and fined $60,000. The defendant filed a notice of appeal on 1/27/14.	issued. 8/3/12: Mandate issued. 3/12/13: Motion to dismiss denied. April 2013: Trial held. 4/24/13: Defendant convicted on all counts. 6/14/13: Motions for acquittal and for a new trial filed. 8/15/13: Motions for acquittal and for a new trial denied. 1/8/14: Defendant sentenced. 1/27/14: Notice of appeal filed.
Computer Fraud and Abuse Act ("CFAA")	*United States v. Auernheimer*, No. 13-1816 (3d. Cir. 3/19/14)	Conviction Overturned	The Third Circuit overturned the conviction of prominent "grey hat" hacker Andrew Auernheimer, holding that venue in the District of New Jersey had been improper because AT&T had no computers located in that jurisdiction and no action was taken with the data in that jurisdiction. Auernheimer had been convicted of violating the CFAA after he wrote a script attacking AT&T's servers and collected thousands of email addresses that were later published on Gawker.com. On appeal, in addition to venue, Auernheimer argued that his actions were not in violation of the CFAA because the data was publicly available on the Internet on an unprotected public webpage. The appellate court did not rule on the merits of Auernheimer's substantive arguments on appeal.	4/11/14: Conviction overturned.
Computer Fraud and Abuse Act ("CFAA") Electronic	*In re iPhone/iPad Application Consumer Privacy Litigation*, No. 5:11-md-02250-LHK	Amended Consolidated Complaint Filed Motion to Dismiss	According to a series of class action complaints consolidated and being heard in the Northern District of California, Apple knowingly allowed millions of users of its iPad and iPhone products to download applications that secretly sent their personal information, including location data, to third-party marketers in violation of the CFAA. Apple had recently come under scrutiny	11/22/11: Amended consolidated complaint filed. 6/12/12: Motion to dismiss

Communications Privacy Act ("ECPA") Stored Communications Act ("SCA")	(N.D. Cal. 11/25/13)	Granted in Part, Denied in Part Third Amended Complaint Filed Motion for Summary Judgment Granted	for allegedly tracking users and collecting their location data. The court granted in part Apple's motion to dismiss, dismissing the claims filed under the SCA, the CFAA, the Wiretap Act, and the California state constitution, as well as state law claims for trespass, conversion, and unjust enrichment. Some claims were left intact, including claims brought under California's Consumer Legal Remedies Act and Unfair Competition Law. The SCA claim was dismissed as the court held iPhones are not facilities through which an electronic communications service is provided; the CFAA claim was dismissed because plaintiffs' voluntary installation of the app negated the "without authorization" elements of the law; and the Wiretap Act claim was dismissed because automatically generated geolocation data is not "content" within the statute, as it is created without the user's intent. The plaintiffs filed a second amended complaint on 7/3/12, and then a third amended complaint on 10/4/12. The third amended complaint asserts claims under California's Consumer Legal Remedies Act and Unfair Competition Act, but also restates the previously dismissed SCA claim on behalf of different plaintiffs. Apple answered the complaint on 11/2/12, and filed a motion for summary judgment on 12/14/12. On 3/7/13, the court denied Apple's motion for summary judgment on procedural grounds, finding that Apple had failed to comply with its discovery obligations and prohibiting it from filing another summary judgment motion until it complies to the court's satisfaction. Apple re-filed its motion for summary judgment on 5/17/13. On 11/25/13, the court granted Apple's motion for summary judgment on the grounds that plaintiffs lacked standing to pursue their claims because they failed to allege actual reliance on Apple's alleged misrepresentations.	granted in part, without leave to amend, and denied in part. 7/3/12: Second amended complaint filed. 10/4/12: Third amended complaint filed. 11/2/12: Apple answer filed. 3/7/13: Summary judgment denied. 11/25/13: Summary judgment granted.
Computer Fraud and Abuse Act ("CFAA") Electronic Communications Privacy Act ("ECPA") Stored Communications Act ("SCA")	*Opperman v. Path, Inc.*, No. 4:13-cv-00453 (N.D. Cal. 1/15/13) *Hernandez v. Path, Inc.*, No. 12-cv-01515 (N.D. Cal. 1/4/13) *In re Apple iDevice Address Book Litigation*, No. 13-cv-453 (N.D. Cal.	Motion to Dismiss Granted (*Opperman*) Case Transferred (*Opperman*) Second Amended Complaint Filed (*Opperman*, *Hernandez*) Motions to Sever Denied	A class action lawsuit was filed against 18 mobile app development companies alleging that their apps steal consumers' mobile address book data without their knowledge or permission in violation of the CFAA (*Opperman*). Those sued include Apple, Electronic Arts, Facebook, Foursquare, Twitter, and Yelp. The suit followed a story in *The New York Times* citing a 2011 study that over 10% of the free apps in the Apple store can access the contacts of the person who downloads the app. Several of the app developers sought to sever the individual claims against them, but the court denied their motions, holding that "Apple's role in marketing, testing, reviewing, and distributing" the various apps made it appropriate to hear the claims together. A similar lawsuit was filed on 3/26/12 against Path, alleging violations of	3/12/12: Complaint filed (*Opperman*). 3/26/12: Complaint filed (*Hernandez*) 10/19/12: Motion to dismiss granted in part (*Hernandez*). 9/3/13: Consolidated class complaint filed. 10/18/13: Motions to

	9/3/13)		ECPA, SCA, and California state law (*Hernandez*). The court granted Path's motion to dismiss in part, rejecting the plaintiff's ECPA and SCA claims but granting leave to amend out of "an abundance of caution." The court later consolidated the two cases along with several other similar cases, which are now being tried together. On 9/3/13, the lead plaintiffs' counsel filed a consolidated class complaint setting forth claims under California statutory law and common law tort theories along with alleged violations of CFAA and ECPA. Multiple motions to dismiss the consolidated class complaint were filed on 10/18/13, which remain pending before the court.	dismiss filed.
Data Breach Health Information	*Tabata v. Charleston Area Med. Ctr. Inc.*, No. C-524 (W. Va. Cir. Ct. 6/26/13)	Complaint Filed Motion to Dismiss Denied Appeal Filed	A class of 3,655 current and former patients of a West Virginia hospital filed a complaint in state court over the hospital's alleged exposure of their personal and medical information on an unsecured website. The complaint alleges that a hospital database created by a contractor "had been accessible and publicized on the Internet since September of 2010." The exposed records included the names, contact details, Social Security numbers, birth dates, and the protected health information of patients. The complaint asserts tort claims of breach of duty of confidentiality, intrusion upon seclusion, unreasonable publicity with respect to the plaintiffs' personal lives, invasion of privacy, and negligence. The defendant filed a motion to dismiss, which has been denied. On 6/24/13, the court denied the plaintiffs' motion for class certification. Plaintiffs have filed an appeal with the West Virginia Supreme Court of Appeals. The case has been fully briefed and oral argument will be heard on 4/23/14.	3/30/11: Complaint filed. 12/30/11: Amended class action complaint filed. 3/1/12: Motion to dismiss filed. 8/22/12: Motion to dismiss denied. 6/24/13: Motion for class certification denied. 6/26/13: Notice of appeal. 4/23/14: Oral argument scheduled.
Data Breach Privacy Act of 1974 Fair Credit Reporting Act ("FCRA")	*In re Science Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, No. 12-mc-347 (D.D.C. 11/15/12)	Complaint Filed Consolidated Amended Complaint Filed Motions to Dismiss Filed	On 10/11/11, a class action lawsuit was filed in response to the breach of computer backup tapes containing the personal information of nearly five million current and former U.S. soldiers. The complaint alleged that Tricare, a health insurance provider for military personnel and the Defense Department, failed to encrypt the data and "intentionally, willfully, and recklessly" allowed an untrained individual to access and take the information out of the premises. The backup tapes were subsequently stolen from the employee's car. The stolen data included Social Security numbers, addresses, and phone numbers, in addition to health assets, such as clinical notes, lab test reports, and prescription information. The suit is requesting $1,000 per affected individual. The consolidated complaint alleges claims under the Administrative Procedures Act, the Privacy Act of 1974, and the	10/11/11: Complaint filed. 6/20/12: Cases consolidated. 10/1/12: Consolidated amended complaint filed. 11/15/12: Motions to dismiss filed.

			Fair Credit Reporting Act, along with various state statutory and common law claims. The defendants filed a motion to dismiss on 11/15/12, which has been fully briefed and remains pending before the court. The case was reassigned to a new judge in early 2014 after the previous judge, Hon. Robert L. Wilkins, was elevated to the U.S. Court of Appeals for the D.C. Circuit.	
Data Breach Health Information	*In re Sutter Med. Info. Cases*, No. JCCP 4698 (Cal. Super. Ct. 12/10/12) *Sutter Health v. Super. Ct.*, C072591 (Cal. Ct. App. 3d Dist. 4/30/13)	Complaints Filed Order Granting Coordination Filed Amended Consolidated Complaint Filed Motion to Strike/Demurrer Filed Case Stayed Appellate Briefs Filed	A large group of patients of Sutter Health whose medical information was compromised following the theft of an unencrypted computer have filed class action complaints against the company alleging it violated California law by failing to adequately protect personal health records. The first part of the group comprises 3.3 million people whose names, addresses, dates of birth, contact information, and medical account numbers were compromised. A further 943,000 people additionally had their personal medical records compromised as well. In addition to injunctive relief, the complaint asks the court to award individual class members $1,000 in statutory damages for each violation of the medical records statute. On 2/17/12, the Judicial Council of California decided that this case, along with 12 others, will be coordinated from Superior Court in Sacramento County. An amended consolidated master class action complaint has been filed, and defendants have filed motions to strike portions of it and a demurrer as to the primary claims within it. On 11/29/12, the defendants filed a petition in the California Court of Appeals seeking resolution of a number of controlling questions of state law. On 1/17/13, the appellate court issued a writ of mandate staying the trial court action and requesting further merits briefing from the parties. Briefs filed in April 2013 remain under the court's consideration.	11/18/11: Complaint filed. 2/17/12: Order granting coordination filed. 5/4/12: Consolidated master class action complaint filed. 11/1/12: Amended consolidated master class action complaint filed. 12/10/12: Motion to strike/demurrer filed. 1/17/13: Appellate writ of mandate issued. April 2013: Appellate briefs filed.
Data Breach	*In re LinkedIn User Privacy Litigation*, No. 12-03088 (N.D. Cal. 3/28/14)	Order Granting Motion to Consolidate Amended Class Complaint Filed Motion to Dismiss Granted Second Amended	Following a breach that allegedly left 6.5 million LinkedIn users' passwords publicly accessible, four class actions lawsuits were filed. The cases have been consolidated into one action before a single district court in California. An amended consolidated class complaint alleges that LinkedIn used insufficient encryption methods to secure password information, deviating from industry standards and violating its own terms of service. The plaintiffs – limited to "premium" LinkedIn members – allege a variety of contract and tort claims, as well as a claim under California's Unfair Competition Law ("UCL"). LinkedIn filed a motion to dismiss, arguing that the plaintiffs have not suffered any cognizable harm sufficient to confer standing. On 3/6/13,	8/29/12: Motion to consolidate granted. 9/19/12: Consolidated class complaint filed. 11/26/12: Amended complaint filed. 12/20/12: Motion to dismiss filed.

		Complaint Filed Motion to Dismiss Filed Motion to Dismiss Granted in Part	the court granted the motion to dismiss. In dismissing the complaint, the court held that the plaintiffs' theory of economic harm to confer standing suffered from four flaws: (1) the privacy policy applies to all users, not just premium members, so premium members have not paid for the promises made in that policy; (2) plaintiffs did not allege that they actually read the policy, therefore precluding a finding that they relied on any alleged misrepresentation; (3) any economic harm resulting from the plaintiffs' breach of contract claims would have occurred prior to the breach; and (4) other than overpaying for a "defective" product, plaintiffs had not shown how they suffered any actual harm under a products liability theory. The court granted leave to amend, however, and on 4/30/13, plaintiffs filed a second amended complaint. LinkedIn filed a motion to dismiss on 6/13/13. The court partially granted LinkedIn's motion to dismiss, leaving intact plaintiff's fraudulent business practices claim that misrepresentations by LinkedIn about its premium subscription caused plaintiffs to suffer economic injury.	3/6/13: Motion to dismiss granted. 4/30/13: Second amended complaint filed. 6/13/13: Motion to dismiss filed. 3/28/14: Motion to dismiss granted in part.
Data Breach	*In re Target Corp. Customer Data Security Breach Litig.*, No. 0-14-md-02522 (D. Minn. 4/3/14)	Cases Consolidated	In response to the large-scale data breach affecting Target retail stores uncovered in mid-December 2013, plaintiffs across the country filed at least 33 actions that have now been consolidated in the District of Minnesota. A consolidated complaint has not yet been filed.	4/3/14: Cases consolidated
Data Breach Health Information Health Insurance Portability and Accountability Act ("HIPAA")	*Abdale v. North Shore-Long Island Jewish Health Sys., Inc.*, No 13-cv-01238 (E.D.N.Y. 6/10/13)	Complaint Filed Motion to Dismiss Filed Motion to Remand Filed	A proposed class action seeks $50 million in punitive damages following the theft of medical records of over 900 patients of a New York hospital by multiple thieves as part of an organized identity theft ring. The stolen information was then used to file fraudulent tax returns, open unauthorized credit card accounts, and make unauthorized purchases at a variety of retailers. Two men unrelated to the hospital have pled guilty to multiple felony charges stemming from the breach. The proposed class complaint asserts various state law claims, including claims for negligence per se based on violations of the hospital's obligations under HIPAA and the HITECH Act. The hospital removed the case to federal court on 3/8/13, then filed a motion to dismiss on 4/16/13, arguing that plaintiffs had failed to allege a cognizable injury or explain how the breach was caused by the hospital's conduct. The motion is now pending before the court. On 6/10/13, plaintiffs filed a motion to remand the case to state court. That motion has been fully briefed and is also pending before the court.	2/5/13: Complaint filed. 3/8/13: Case removed to federal court. 4/16/13: Motion to dismiss filed. 6/10/13: Motion to remand filed.

COURTS (continued)

Data Breach	*Resnick v. AvMed Inc.*, No. 1:10-cv-24513 (S.D. Fla. 2/28/14)		A federal judge has approved an unprecedented settlement in a data breach class action suit against a health insurance company that allows plaintiffs who did *not* have their identities stolen to claim settlement funds. The settlement requires the company to fully reimburse class members who had their identities stolen for costs incurred, and to pay each class member $10 for every year they purchased insurance, up to three years. AvMed must also implement new security measures. Plaintiffs had alleged that AvMed's failure to develop and implement proper data security measures allowed for the theft of two laptops containing customers' personal and medical information.	2/28/14: Final settlement approval granted.
Data Breach	*Express Scripts, Inc. v. Ernst & Young LLP*, No. 13DL-CC00537 (Mo. Cir. Ct. 12/30/13)	Complaint Filed Motion to Dismiss Denied	Express Scripts has alleged that an Ernst & Young partner stole 20,000 pages of trade secrets and proprietary data while working as a consultant for the company, using the physical and computer security credentials of other employees to gain unauthorized access to internal databases. The complaint further alleges that the partner involved used the stolen data to advise a competitor firm to Express Scripts. The complaint asserts various state law claims and seeks relief, including punitive damages. On 3/6/13, E&Y filed a motion to dismiss, which remains pending before the court, admitting that its employee exercised poor judgment but arguing that none of the data was improperly used and that Express Scripts' security standards were insufficient. On 12/5/13, the court denied E&Y's motion to dismiss and issued a preliminary injunction requiring E&Y to protect Express Scripts' data during the pendency of the litigation. The court also rejected E&Y's demands to submit the dispute to arbitration.	2/14/13: Complaint filed. 3/6/13: Motion to dismiss filed. 12/5/13: Motion to dismiss denied; preliminary injunction issued. 12/30/13: Answer filed.
Data Privacy	*Yuncker v. Pandora Media, Inc.*, No. 11-cv-3113 (N.D. Cal. 3/10/14)	Amended Complaint Filed Motion to Dismiss Granted in Part and Denied in Part	A group of Pandora Internet radio users has filed an amended complaint alleging that the company misuses their personal information following an order dismissing their original complaint in which the judge ruled they had failed to establish any harm caused by Pandora's conduct. The amended complaint alleges violations of California's Unfair Competition Law and state constitutional right to privacy based on Pandora's practice of disseminating users' information to third-party advertising libraries. Plaintiffs have augmented their description of their alleged injuries, arguing that the market for private consumer information gives that information concrete economic value. Pandora filed a motion to dismiss on 5/30/13, which remains pending before the court. On 3/10/14, the court granted in part and denied in part Pandora's motion to dismiss. The court denied the motion to dismiss with respect to the standing, UCL, and breach of privacy policy claims because plaintiffs had alleged facts sufficient to plead these claims, but noted that the plaintiffs will have an uphill battle proving them. The court	5/9/13: Amended complaint filed. 3/10/14: Motion to dismiss partially granted.

			affirmed its prior dismissal of the plaintiffs' constitutional claims.	
Data Privacy	*Advanced Career Techs. v. Does*, No. 13-cv-304 (D. Colo. 3/11/13)	Motion for Expedited Discovery Granted Amended Complaint Filed	A federal magistrate judge has ruled that a plaintiff is entitled to expedited discovery to determine the identities of ten unknown individuals who allegedly posted libelous entries on a blog hosted by Blogspot (owned by Google). Finding that the plaintiff had no other feasible means of identifying the anonymous posters, the court granted permission to issue third party subpoenas on Google and the blog's operator to seek each defendant's name, address, telephone number, email address, and IP address. The operator unsuccessfully sought to quash the subpoena but has not yet produced any identifying information about posters on the blog. Additionally, plaintiff notified the court that a large amount of posts and other information has been deleted from the blog in question and explained that it is considering pursuing a motion to compel against the operator, or a motion for contempt if the evidence was permanently destroyed. Google has not yet complied with the subpoena against it, although the parties remain in discussions. On 3/25/14, plaintiff filed an amended complaint including claims against the blog operator in his individual capacity. In a contemporaneous status report, plaintiffs reported that they still have not been able to establish the identities of the ten posters.	3/11/13: Motion for expedited discovery granted. 3/25/14: Amended complaint filed.
Data Privacy	*Pirozzi v. Apple, Inc.*, No. 12-cv-1529 (N.D. Cal. 8/5/13)	Motion to Dismiss Denied in Part	A federal district court has refused to dismiss claims that Apple violated California state law by allowing third-party apps to access and upload data from other apps. Apple had moved to dismiss, arguing that the plaintiff (an iPhone purchaser) could not establish a cognizable injury. The court disagreed, holding that the plaintiff established an injury sufficient for Article III standing based on her reliance on Apple's representations regarding the phone's data security and her alleged subsequent discovery that apps were, in fact, accessing data from other apps. These representations included statements on Apple's website such as "All apps run in a safe environment, so a website or app can't access data from other apps" and "To guard your privacy, apps requesting location information must get your permission first."	8/5/13: Motion to dismiss denied in part.
Data Privacy Children's Online Privacy Protection Act ("COPPA")	*Fraley v. Facebook, Inc.*, No. 11-cv-1726 (N.D. Cal. 8/26/13) *Batman v. Facebook,*	Settlement Approved	A group of Facebook users sued the social networking service in 2011 after it implemented its "Sponsored Stories" feature. This feature allows advertisers to pay Facebook to display advertisements that feature the name or likeness of a user's "friend" who has "liked" that company, ostensibly giving the appearance that the friend endorses the product and thereby making the advertisement more attractive to the user. On 8/26/13, a federal judge	8/26/13: Settlement approved *(Fraley)*. 9/09/13: Notice of appeal filed *(Batman)*. 3/14/14: Appellants' briefs

	Inc., No. 13-16819 (9th Cir. 3/20/14) *C.M.D. v. Facebook, Inc.*, No. 3:12-cv-01216 (N.D. Cal. 3/26/14)		approved a final settlement between the parties, pursuant to which Facebook will pay damages of over $20 million, improve the notice provided to users about its practices, and adjust its parental consent and privacy settings to enable users to avoid participating in the "Sponsored Stories" feature at all. On 9/09/13, class members filed a notice of appeal of the settlement on a settlement fund distribution point. Some class members objected to the settlement terms because they did not ensure parental consent would be obtained before using a minor's name or image. The lower court dismissed the objection on the ground that it was preempted by COPPA as to minors over the age of 13. As part of the proceedings, the FTC filed a significant amicus brief opposing the position taken by the court on state law preemption by COPPA. The FTC explained that although the lower court's determination was not a decision on the merits, it opposed the lower court's preemption view because there is no indication that COPPA preempts state law privacy protections for people who fall outside the scope of COPPA's coverage, including teenagers over the age of 13. The FTC's explanation effectively leaves room for states to supplement COPPA's coverage with additional privacy laws, as long as they do not conflict with COPPA. Opening briefs have been filed in the case and answers are expected on 5/30/14. Additionally, some class members opted out of the settlement and pursued the suit but only as to the use of minors' names and images (*C.M.D.*). The court granted Facebook's motion to dismiss, explaining that the plaintiffs alleged no legal theory rendering Facebook's terms of use unenforceable, and therefore the plaintiffs gave consent to the use of their names and images when they signed up for Facebook's service regardless of their status as minors.	filed (*Batman*). 3/20/14: FTC amicus brief filed (*Batman*). 3/26/14: Motion to dismiss granted (*C.M.D.*).
Data Security	*In re Bed Bath & Beyond, Inc. ZIP Code Litigation*, No. 13-cv-10639 (D. Mass. 5/15/13)	Complaint Filed Answer Filed	Following the decision of the Supreme Judicial Court of Massachusetts in *Tyler v. Michaels Stores* (see below), which held that Michaels' use of ZIP codes collected for billing purposes but subsequently used for marketing purposes gives rise to a cognizable injury, a similar putative class action lawsuit was filed against Bed Bath & Beyond. The complaint seeks damages of $25 per class member, and proposes a class of all of the retailers' shoppers whose ZIP code information was collected from 3/20/09 onward. Bed Bath & Beyond filed an answer on 5/15/13, and discovery in the case has begun.	3/20/13: Complaint filed. 5/15/13: Answer filed.

COURTS (continued)

Data Security	*FTC v. Wyndham Worldwide Corp.*, No. 13-cv-01887 (D.N.J. 4/26/13)	Complaint Filed Motion to Dismiss Filed Motion to Dismiss Denied	The FTC has filed a complaint against Wyndham alleging failure to take adequate security measures to protect personally identifiable information even after security breaches in 2008 and 2009. Wyndham filed a motion to dismiss on 4/26/13, which the court denied on 4/7/14. The court explained that the FTC has authority to regulate data security without needing to publish formal rules and regulations governing specific data security practices and that the FTC had sufficiently alleged that Wyndham had engaged in unfair and deceptive data security practices. **See the "Federal Agencies" section above for more details on this case.**	6/26/12: Complaint filed. 8/9/12: Amended complaint filed. 4/26/13: Motion to dismiss filed. 4/7/14: Motion to dismiss denied.
Data Security	*Genesco Inc. v. Visa, Inc.*, No. 13-cv-202 (M.D. Tenn. 8/23/13)	Complaint Filed Motion to Dismiss Filed	Apparel marketing giant Genesco has sued Visa to recover over $13 million in fines levied by Visa for Genesco's alleged failure to adhere to Payment Card Information Data Security Standards (PCI DSS) following a 2010 hacking data breach. Visa assessed various fines and fraud recovery costs against Genesco's banks, which in turn withdrew the funds from Genesco accounts. According to the complaint, Genesco was in compliance with PCI DSS but hackers exploited a weakness to capture credit card information. Specifically, at the time of the breach, PCI DSS allowed companies to transmit unencrypted customer payment card data during the payment authorization process, and the hackers captured the data during that authorization process. The complaint asserts various breach of contract claims, as well as a claim for violation of the California Unfair Business Practices Act. On 5/20/13, Visa filed a motion to dismiss, which was denied on 7/18/13. On 8/23/13, Genesco filed a motion for summary judgment on its claims related to the $10,000 in "fines" issued by Visa, but not the $13 million in "assessments" that remain at issue.	3/7/13: Complaint filed. 5/20/13: Motion to dismiss filed. 7/18/13: Motion to dismiss denied. 8/23/13: Motion for summary judgment filed.
Data Security	*Tyler v. Michaels Stores, Inc.*, No. 1:11-cv-10920-WGY (D. Mass. 1/17/14) *Tyler v. Michaels Stores, Inc.*, No. SJC-11145 (Mass. 3/11/13)	Class Action Complaint Dismissed Question Certified Opinion Issued Preliminary Approval of Settlement	On 1/6/12, a federal district court judge in Massachusetts dismissed a putative class action filed against Michaels Stores, Inc. holding that a store's collection of a ZIP code during a credit card transaction did not result in cognizable injury necessary to support the statutory claim. The ruling did state, in a case of first impression, that an individual's ZIP code is protected personal information under a Massachusetts consumer protection statute, Mass. Gen. Laws ch. 93, § 105 , but that the plaintiff failed to demonstrate any cognizable injury as a result of a violation of the Massachusetts statute. The plaintiff had alleged that she was opened up to an increased unreasonable risk of fraud. The ruling noted that the plaintiff did not allege that the ZIP code collection alone exposed her to this increased risk, as the ZIP code had to be combined with other data to identify her address. The court also dismissed an unjust enrichment tort claim and a request for a	5/23/11: Class action complaint filed. 1/6/12: Class action complaint dismissed. 2/10/12: Question certified to the Supreme Judicial Court of Massachusetts. 11/6/12: Oral argument held. 3/11/13: Opinion issued.

			federal declaratory judgment. In dismissing the complaint, the court further noted that the California Supreme Court, in assessing a state statute similar to the Massachusetts law in *Pineda v. Williams-Sonoma Stores Inc.*, 246 P.2d 612 (Cal. 2011), held that legislative history indicated that the California law was broadly aimed at preventing merchants from using information to send unwanted ads to consumers. According to the district court, the Massachusetts legislature was concerned with the narrower goal of stopping potential fraud due to identity theft. Shortly after dismissal, the plaintiff certified the question to the Supreme Judicial Court of Massachusetts. On 3/11/13, the court issued an opinion in which it agreed that ZIP codes are protected under Massachusetts law, but rejected the lower court's reasoning that Massachusetts was only concerned with identity theft, instead ruling that the law aimed to protect consumer privacy as well. Under the court's holding, Michaels' use of ZIP code collected for billing purposes but used for marketing purposes gives rise to a cognizable injury. Like the *Pineda* decision in California, this decision may start a wave of similar class action suits against retailers. (See *In re Bed Beth & Beyond, Inc. ZIP Code Litigation*, above.) The district court case has been reopened in light of the SJC's opinion and discovery is under way. On 2/12/14, the court granted preliminary approval to a proposed settlement, but the terms of the settlement have not yet been made public.	4/29/13: Answer filed. 2/12/14: Preliminary approval of settlement.
Data Security	*LabMD Inc. v. Federal Trade Commission*, No. 13-15267 (11th Cir. 2/18/14) *LabMD Inc. v. Federal Trade Commission*, No 1:13-cv-01787 (D.D.C. 2/19/14)	Administrative Complaint Filed Complaint Filed Petition for Review Filed Ruling on Petition Issued Complaint Withdrawn	In August 2013, the FTC issued an administrative complaint against LabMD, a medical testing laboratory, alleging that the company had engaged in unfair acts or practices under Section 5(a) of the Federal Trade Commission Act by failing to reasonably protect the security of consumers' personal data. Consumers' personal information had been discovered on a file sharing network and in the possession of identity thieves on two separate occasions. The FTC proposed an order requiring LabMD to implement a security program that would be evaluated every two years for the next 20 years and requiring LabMD to notify consumers whose information was or could have been disclosed. On 11/14/13, LabMD filed a complaint in D.C. District Court alleging four claims related to abuse of authority and constitutional violations. LabMD sought a declaratory judgment that the FTC lacks authority to regulate data security and an injunction to prevent the FTC from continuing its administrative action. On 11/18/13, LabMD filed a petition for review with the Eleventh Circuit asking the court to review the FTC's administrative action	11/14/13: Complaint filed. 11/18/13: Petition for review filed. 2/18/14: Ruling on the petition for review issued. 2/19/14: Complaint voluntarily withdrawn.

			proceeding under Section 5 against LabMD. On 2/18/14, the Eleventh Circuit dismissed the petition *sua sponte* for lack of jurisdiction as the court's authority was limited to reviewing FTC orders to cease and desist from anticompetitive acts and practice and no such order had been issued by the FTC in this case. It also noted, without expressing an opinion over jurisdiction, that the district court was the proper venue in which to first bring an Administrative Procedure Act, *ultra vires*, or constitutional claim. Following the Eleventh Circuit's ruling, LabMD voluntarily withdrew its complaint in the D.C. District Court on 2/19/14. The administrative proceeding against LabMD remains pending at the FTC.	
Data Security Data Breach	*Halpain v. Adobe Systems Inc.*, No. 5:13-cv-05226 (N.D. Cal. 4/4/14)	Consolidated Complaint Filed	In 2013, Adobe's network was hacked, allowing the perpetrators to steal customer credit card accounts and personal information and Adobe source code over a several-week period before the breach was detected by independent entities. Customers filed a class action lawsuit against Adobe for failure to implement proper security measures to protect personal information. Plaintiffs seek a declaratory judgment that Adobe did not comply with its contractual security obligations, an injunction requiring Adobe to implement proper security protocols, and restitution for customers who purchased Adobe ColdFusion and Creative Cloud services.	4/4/14: Consolidated class action complaint filed.
Data Security Data Breach Electronic Contracts Fair Credit Reporting Act ("FCRA")	*In re Sony Gaming Networks & Customer Data Security Breach Litig.*, No. 11-md-2258 (S.D. Cal. 1/21/14)	Motion to Dismiss Partially Granted Amended Complaint Filed Motion to Dismiss Partially Granted	In 2011, Sony experienced a large data breach that exposed personal data and credit card accounts for more than 69 million users. This class action lawsuit contends that Sony misrepresented the quality of the protections it used for the systems affected in the breach. A judge disagreed, citing a provision of Sony's privacy policy, stating, "Unfortunately, there is no such thing as perfect security. As a result, although we strive to protect personally identifying information, we cannot ensure or warrant the security of any information transmitted to us through or in connection with our website, Sony Online Services or that we store on our systems or that is stored on our service providers' systems." In ruling, the judge held that this "clear admonitory language" meant "no reasonable consumer could have been deceived" about the state of Sony's protections. The court did, however, leave the door open for plaintiffs to show injury sufficient to confer standing if they could demonstrate actual misuse of the compromised data. On 12/10/12, the plaintiffs filed an amended complaint that contains multiple state law claims. The complaint also alleges willful and negligent violations of FCRA on the basis that Sony provides credit information to	10/11/12: Motion to dismiss partially granted. 12/10/12: Amended complaint filed. 1/21/14: Motion to dismiss partially granted.

			certain Sony subsidiaries and affiliates and violated its obligation under FCRA to sufficiently safeguard its customers' personal information. Sony filed a motion to dismiss on 2/12/13, again asserting that plaintiffs lacked sufficient injury to confer standing and rejecting the characterization of Sony subsidiaries as credit reporting agencies subject to FCRA regulation. On 1/21/14, the court granted in part and denied in part Sony's motion to dismiss. The court dismissed plaintiffs' claims under the FCRA because Sony does not meet the statutory definition of a consumer reporting agency. The court refused to dismiss the plaintiffs' state law claims and rejected Sony's argument that plaintiffs lacked standing, holding that the Supreme Court's recent decision in *Clapper v. Amnesty International* did not create a new standard for the injury-in-fact requirement, and finding that allegations that personal information was collected and then wrongfully disclosed as a result of intrusion was sufficient to allege standing.	
Eavesdropping First Amendment	*State v. Clark*, No. 2014 IL 115776 (Ill. Sup. Ct. 3/20/14) *State v. Melongo*, No. 2014 IL 114852 (Ill. Sup. Ct. 3/20/14)	Opinions Issued (*Clark*, *Melongo*)	In two opinions issued on 3/20/14, the Illinois Supreme Court found that the state's criminal eavesdropping statute is unconstitutional as a violation of the First Amendment. Both cases arose out of situations in which the defendant recorded a conversation with a public official acting within the scope of his or her duty without consent. The court explained that the statute extends beyond legitimately private conversations to criminalize the recording of loud conversations held in public fora, which is innocent conduct because no reasonable expectation of privacy exists for these conversations. The court additionally explained that the statute does not differentiate recordings made without the knowledge of the recorded party from recordings made with the knowledge of the recorded party but without that party's consent. The court in *Melongo* also found that the Illinois statute's provision prohibiting divulging any recording made on a cellphone or other device regardless of consent is unconstitutional. The court explained that because the recording provision of the statute was unconstitutional, the divulging provision must also fail because, under U.S. Supreme Court precedent, a state may not prohibit the disclosure of a legitimately made recording.	3/20/14: Opinions Issued
Electronic Communications Privacy Act ("ECPA") Federal Education Privacy Rights Act	*Fread v. Google, Inc.*, No. 13-cv-1961 (N.D. Cal. 5/16/13)	Complaint Filed	A new class action complaint filed by two university students seeks up to $1 billion in damages against Google for alleged violations of ECPA. The students claim that Google illegally harvests the content of emails sent and received through their school's email service, which is provided via Google's Apps for Education program. Google's acquisition of content keywords and other metadata allows the company to avoid "traffic acquisition costs," thus	4/29/13: Complaint filed. 5/16/13: Case consolidated.

("FERPA")			rendering the information highly valuable, according to the complaint, although the complaint does not make clear how Google actually uses any of the acquired information. Additionally, plaintiffs claim that Google falsely classifies itself as a "school official" authorized to access school records under FERPA in its contract with the plaintiffs' schools. The suit seeks to create a potential class of over 100,000 users of Google's education apps and to recover a statutory penalty of up to $10,000 per violation. On 5/16/13, the case was consolidated with other similar complaints into an ongoing consolidated action in the Northern District of California. **See *In re Google Inc. Gmail Litigation* below for more information.**	
Electronic Communications Privacy Act ("ECPA")	*Brinkman v. Google Inc.*, No. 12-6699 (E.D. Pa. 2/4/13) *In re Google Inc. Gmail Litigation*, No. 13-md-02430 (N.D. Cal. 10/1/13)	Complaint Filed Consolidated Complaint Filed Motion to Dismiss Granted in Part, Denied in Part Amended Consolidated Complaint Filed	Google faces a consolidated class action seeking over a billion dollars in damages based on allegations that Google intercepts incoming emails to Google email account holders for advertising and marketing purposes in violation of federal and state wiretap laws. Combined, the consolidated class consists of all Gmail users from 2008 onward. A consolidated complaint was filed on 5/16/13. On 6/13/13, Google filed a motion to dismiss, arguing *inter alia* that ECPA should not apply because any interceptions that occurred fall within ECPA's "ordinary course of business" exception and that users had consented to any interceptions by agreeing to Google's terms of service. The court granted in part and dismissed in part the motion to dismiss on 9/26/13, rejecting Google's arguments regarding ECPA. The court held that the "ordinary course of business" exception is a narrow one. On the issue of consent, the court ruled that although the terms of service notified users that their emails might be monitored, they did not state that monitoring would occur for the specific purpose of advertising and marketing uses and therefore users could not have consented to the interceptions at issue. The court also rejected Google's argument that Gmail users have no expectation of privacy in the contents of their messages. The court dismissed certain state law claims, but gave plaintiffs leave to amend. Plaintiffs filed an amended complaint on 10/1/13. Defendants filed an answer to plaintiffs amended complaint on 11/21/13. On 3/18/14, the court denied plaintiffs' request to certify seven classes with prejudice because the individual issues predominated the common issues of fact.	11/30/12: Complaint filed. 4/1/13: Case consolidated and transferred (*Brinkman*). 5/16/13: Consolidated complaint filed. 6/13/13: Motion to dismiss filed. 9/26/13: Motion to dismiss granted in part and denied in part. 10/1/13: Amended consolidated complaint filed. 11/21/13: Answer filed. 3/18/14: Class certification motion denied.

COURTS (continued)

Electronic Communications Privacy Act ("ECPA")	*Kevranian v. Yahoo! Inc.*, No. 13-cv-4547 (N.D. Cal. 1/9/14)	Complaint Filed Case Voluntarily Dismissed	In a very similar case to the Google litigation above, a group of non-Yahoo! users has sued Yahoo! for violating federal and state wiretap laws by scanning emails sent to Yahoo! users by non-users in order to target advertisements. The complaint seeks statutory damages along with an order enjoining Yahoo! from continuing to monitor incoming emails from non-users. Parties stipulated to dismiss the case and the court approved the dismissal on 1/9/14.	10/2/13: Complaint filed. 1/9/14: Case voluntarily dismissed.
Electronic Communications Privacy Act ("ECPA") California Invasion of Privacy Act	*Campbell v. Facebook, Inc.*, No. 4:13-cv-05996 (N.D. Cal. 12/30/14)	Complaint Filed	On 12/30/13, plaintiffs filed a proposed class action suit against Facebook for mining user data from private messages and sharing the information with third-party advertisers, marketers, and data aggregators without user consent. Plaintiffs alleged that Facebook violated ECPA and California privacy law by intentionally intercepting the contents of users' private messages, which are electronic communications sent using the service, during transmission and used the substance of the messages for advertising purposes in violation of its user agreements. Facebook has not yet filed a response to plaintiff's complaint.	12/30/14: Complaint filed.
Fair Credit Reporting Act ("FCRA")	*Bickley v. Dish Network, LLC*, No. 3:10-cv-00678 (W.D. Ky. 7/12/13) *Bickley v. Dish Network LLC*, No. 13-5956 (6th Cir. 9/10/13)	Summary Judgment Granted	A district court judge ruled that Dish Network did not violate the FCRA when it pulled credit reports for a consumer for a new account initiated by an identity thief who used the consumer's Social Security number. Despite the fact that the plaintiff himself did not authorize the inquiry, the court found that Dish had a legitimate purpose to seek the information under the FCRA. The court held that Dish lacked the requisite culpability to be found liable for even negligent violation of the FCRA, since it followed all normal procedures for verifying the consumer's identity and accessing his credit reports. On 11/12/12, the plaintiff filed a motion for reconsideration, which the court denied on 5/8/13. The plaintiff has appealed to the Sixth Circuit. The case has been fully briefed but no oral argument has been scheduled.	11/3/10: Complaint filed. 11/2/12: Summary judgment granted. 11/12/12: Motion for reconsideration filed. 5/8/13: Motion for reconsideration denied. 7/12/13: Notice of appeal filed. 9/10/13: Opening brief on appeal filed.
Fair and Accurate Credit Transactions Act ("FACTA") Fair Credit Reporting Act ("FCRA")	*Crupar-Weinmann v. Paris Baguette USA Inc.*, No. 1:13-cv-07013 (S.D.N.Y. 1/16/14)	Case Dismissed	A district court has dismissed a putative class action suit against the defendant for willfully violating FACTA by printing customers' credit card expiration dates on their receipts along with their properly redacted credit card numbers. The defendant had moved for dismissal on 11/18/13, arguing that plaintiff failed to allege sufficient facts to show a willful violation of the statute. In its dismissal order the court stated it would issue an opinion on the matter at a later date; the opinion has not yet been released.	11/18/13: Motion to dismiss filed. 1/16/14: Motion to dismiss granted.

COURTS (continued)

Fair and Accurate Credit Transactions Act ("FACTA") Fair Credit Reporting Act ("FCRA")	*Miller v. Sw. Airlines Co.*, No. 3:12-cv-05978 (N.D. Cal. 3/21/14) *Lumos v. Sw. Airlines Co.*, No. 3:13-cv-01429 (N.D. Cal. 3/21/14)	Settlement Approved	On 3/21/14, a federal judge approved a $1.1 million settlement resolving two consolidated class action suits against Southwest Airlines for willfully violating FACTA by printing customers' credit card expiration dates on their receipts. Under FACTA, a vendor can print either the last five digits of a credit card number or the card's expiration date, but not both.	3/21/14: Court approves settlement.
First Amendment	*Hadeed Carpet Cleaning Inc. v. John Doe #1*, No. 0116-13-4 (Va. Ct. App. 1/7/14)	Opinion Issued	The Virginia Court of Appeals has held that Yelp must reveal the identity of individuals who posted negative reviews on Yelp's site under Virginia's unmasking statute despite Yelp's argument that the reviewers' identities were protected by the First Amendment. The court explained that because the First Amendment does not protect speech that is defamatory and limits the right to speak anonymously when speech is commercial, and because there was no clear and palpable infirmity with Virginia's law, it declined to find the law unconstitutional. The court also refused to be persuaded by case law from other jurisdictions. The court found that because the plaintiff had complied with Virginia's unmasking law, the subpoena against Yelp to identify the negative reviewers was enforceable.	1/7/14: Opinion issued.
Fourth Amendment	*State v. Hinton*, No. 87663 (Wa. 5/7/13) *State v. Roden*, No. 87669 (Wa. 5/7/13)	Appellate Briefs Filed Opinions Issued (*Hinton*, *Roden*)	The Washington Supreme Court issued opinions in two cases that may have significant implications for the privacy of text messages. In both cases, a detective acquired the cell phone of a drug dealer who had previously been arrested; the defendants sent multiple texts to the phone indicating interest in purchasing drugs, which the detective read and replied to without a warrant, posing as the dealer, ultimately arresting the defendants at arranged meetings. A lower appeals court affirmed both convictions, holding that the defendants' Fourth Amendment privacy interest in the messages terminated when the messages were sent. The Supreme Court overturned the appeals court and held that the defendant's text massages were "private communications" that had been "intercepted" within the meaning of the statute. The court analogized text messages to phone conversations and emails and explained that the defendant had a reasonable subjective intent that the messages would remain private notwithstanding the potential for interception by an unintended party. The court also differentiated between the federal and Washington state privacy statutory schemes, explaining that while the federal scheme is technology-specific, Washington's statute is not based on technical distinctions, and therefore by manipulating the phone to produce defendant's text messages, the officer "intercepted" the defendant's	4/8/13: EFF amicus brief filed (*Hinton*, *Roden*). 5/7/13: Oral argument heard. 2/27/14: Opinions issued (*Hinton*, *Roden*).

			text messages. The Court did not reach the Fourth Amendment issues in the case.	
Massachusetts Unfair Trade Practices Act	*Christensen v. Apple Inc.*, No. 1:14-cv-10100 (D. Mass.1/15/14)	Complaint Filed Motion to Dismiss Filed	Plaintiffs filed a proposed class action suit in Massachusetts federal district court alleging that Apple violated Massachusetts's Unfair Trade Practices Act by making customers believe they must provide their ZIP code in connection with making a credit card purchase from Apple. Plaintiffs claimed they were injured because Apple sold their personal information to third parties and because they received unwanted marketing material from Apple. Apple filed an answer to the complaint on 3/13/14 with seven affirmative defenses, including arguing that plaintiffs lacked standing because they suffered no injury. Apple denied selling customer ZIP codes to third parties and using the ZIP codes to send marketing materials to plaintiffs.	1/15/14: Complaint filed. 3/13/14: Answer filed.
Michigan Video Rental Privacy Act	*Deacon v. Pandora Media, Inc.*, No. 11-4674 (N.D. Cal. 9/28/12) *Deacon v. Pandora Media, Inc.*, No. 12-17734 (9th Cir. 8/2/13)	Complaint Filed Case Dismissed Notice of Appeal Filed Briefs Filed	Plaintiff filed a lawsuit against Pandora alleging violations of a 1988 Michigan state law that imposed fines for disclosing a customer's purchase or rental histories relating to videos, books, or sound recordings (similar to the federal VPPA). The plaintiff argued that Pandora violated the law by making profile pages of its users (containing user names and music preferences) visible to others, and compounded the violation when it integrated Facebook sharing features without notifying users. Pandora argued that it doesn't sell, rent, or lend music, but that it streams music. The court agreed with Pandora and defined "lending" as the act of receiving something temporarily for use and then returning it, but Pandora's technology temporarily creates a new file and then deletes it (rather than returning it). Although the plaintiff was given leave to re-file and argue that streaming is equivalent to lending, he instead filed a notice of appeal to the Ninth Circuit on 12/12/12. Briefs on appeal have been filed, but oral argument has not yet been scheduled.	9/20/11: Complaint filed. 11/28/11: Motion to dismiss filed. 9/28/12: Motion to dismiss granted. 12/12/12: Notice of appeal filed. 4/22/13: Opening brief filed. 5/22/13: Opposition brief filed. 8/2/13: Reply brief filed.
New Jersey Wiretap Act	*State v. Ates*, No. 070926 (N.J. 3/18/14)	Opinion Issued	The New Jersey Supreme Court has upheld the constitutionality of the state's Wiretapping and Electronic Surveillance Control Act, which is modeled after the federal Wiretap Act. The New Jersey law allows a judicial wiretap order to be executed "at any point of interception within the jurisdiction of an investigative or law enforcement officer executing the order." The point of interception is the location where the listening officer is at the time of interception, which must be within New Jersey's borders. The defendant, who was on trial for murder, argued that the law was unconstitutional because it allows police to intercept conversations between people located outside of the state's borders. The court explained that many federal and	3/18/14: Opinion issued.

			state courts interpreting wiretap statutes have allowed judges to authorize wiretaps for phones outside of the court's jurisdiction when the point of interception is located within the jurisdiction, which is necessary for practical and efficiency reasons due to the mobility of cellphones. The court also explained that judges in the states where the phone was located and monitored would have to review the wiretap application to ensure there was an adequate basis for the order and that the application must meet Title III standards to ensure that the individual's privacy rights were protected.	
Stored Communications Act ("SCA")	*Gaos v. Google Inc.*, No. 5:10-cv-04809-EJD (N.D. Cal. 4/30/13) *In re Google Referrer Header Privacy Litigation*, No. 10-cv-4809 (N.D. Cal 3/25/14)	Motion to Dismiss Partially Denied Amended Complaint Filed Motion to Dismiss Filed Preliminary Settlement Reached	Google has intentionally structured its search engine such that when a user searches for something, and then clicks on a search result, the operator of the website clicked on will be aware of the terms for which the user searched. The plaintiff sued, stating that this was a violation of the SCA and other established law. The court partially granted Google's motion to dismiss as to tort claims, but left intact the SCA claim. Google had argued that the plaintiff lacked Article III standing because no injury was caused through its disclosure of the plaintiff's search terms to websites the plaintiff clicked on that were listed in her search results. The court disagreed, stating that Google's alleged violations of her rights under the SCA were sufficient to confer standing by themselves. Google did not move to dismiss on the merits, and so the court did not address that issue. The plaintiff amended its complaint, and a second motion to dismiss is pending before the court. On 4/30/13, the court denied the motion to dismiss as moot, instead consolidating a similar case into *Gaos*. Complaints have not yet been filed in the consolidated action. On 7/19/13, the plaintiff filed a motion for preliminary approval of a proposed settlement. Under the terms of the proposed settlement, Google would make a cash payment of $8.5 million and would agree to post disclosures on its website notifying users whether and the extent to which search queries are transmitted to third parties. On 3/25/14, the court granted preliminary approval of the settlement.	3/29/12: Motion to dismiss partially granted and partially denied. 5/1/12: Second amended complaint filed. 6/15/12: Motion to dismiss filed. 4/30/13: Motion to dismiss denied as moot; case consolidated. 7/19/13: Motion for preliminary approval of settlement filed. 3/25/14: Motion for preliminary approval of settlement granted.
Stored Communications Act ("SCA")	*In re Facebook Privacy Litig.*, No. 5:10-cv-02389-JW (N.D. Cal. 11/22/11) *Robertson v. Facebook, Inc.*, No. 12-15619 (9th Cir.	Complaint Dismissed Notice of Appeal Filed	The court dismissed an amended class action complaint alleging that Facebook unlawfully disclosed users' personal data to the website's advertising partners given that the court did not believe that the complaint sufficiently alleged that Facebook is a remote computing service ("RCS") provider under the SCA. The complaint alleged that Facebook, without user consent, shared personal data with third-party advertisers through the use of "Referrer Headers" that Facebook allegedly sends to advertisers when users click on ads. The court concluded that Facebook was not an RCS, as the term refers to a third party that processes or stores data for subscribers. The	11/22/11: Complaint dismissed. 3/22/12: Notice of appeal filed. 8/13/12: Appellant's opening brief filed. 9/26/12: Appellee's

	1/17/14)		court said that Facebook could not have been acting as a RCS because the communications at issue were requests to be connected to advertisements, not data to be processed or stored. The court also concluded that the loss in value of personal information could not constitute damages to support the plaintiffs' claim. On 3/21/12, representative plaintiff Robertson filed an appeal to the Ninth Circuit. Opening briefs were filed 8/13/12 and 9/26/12, and a reply brief was filed on 11/19/12. Oral argument was heard on 01/17/14.	opening brief filed. 11/19/12: Appellant's reply brief filed. 1/17/14: Oral argument heard.
Stored Communications Act ("SCA")	*CTIA v. Telecomms. Reg. Bd. of Puerto Rico*, No. 3:12-cv-01104-FAB-BJM (D.P.R. 8/2/12) *CTIA v. Telecomms. Reg. Bd. of Puerto Rico*, No. 12-2427 (1st Cir. 11/5/13)	Order Denying Motion to Dismiss Opinion Issued Notice of Appeal Filed Briefs on Appeal Filed	A district court judge held that the SCA preempts a law in Puerto Rico that would require CTIA, a wireless industry trade association, to disclose customer information. The SCA requires a government entity to subpoena the disclosure of customer information, while the law at issue permits disclosure without any such process. On 10/18/12, the district court approved a magistrate's report and recommendation, granting a permanent injunction that enjoins the defendant from enforcing Puerto Rico's law. The defendant has filed a notice of appeal, which is currently pending. Briefs have been filed; oral argument was heard on 11/5/13.	8/2/12: Motion to dismiss denied. 10/1/12: Magistrate's Report & Recommendation issued. 10/18/12: Opinion issued. 11/2/12: Notice of appeal filed. 2/28/13: Opening brief filed. 4/2/13: Opposition brief filed. 4/16/13: Reply brief filed. 11/5/13: Oral argument heard.
Stored Communications Act ("SCA")	*Garcia v. City of Laredo*, No. 11-41118 (5th Cir. 1/16/13) *Garcia v. City of Laredo*, No. 12-1264 (U.S. 6/24/13)	Opinion Issued Petition for Writ of Certiorari Denied	The Fifth Circuit held that the SCA does not apply to text messages, images, and video files stored on a personal cell phone. A police dispatcher had her cell phone taken without her consent from her footlocker by a police officer's wife, who then turned it over to police department investigators. The investigators reviewed text messages, images, and video files stored on the phone, and downloaded several of the images to an external storage device. The court held that a cell phone is not a "facility" subject to the SCA and that, even if it was, text messages and images would not constitute "electronic storage" under the law. A subsequent petition for rehearing *en banc* was denied. On 4/16/13, Garcia filed a petition for a writ of certiorari	12/12/12: Opinion issued. 1/16/13: Petition for rehearing *en banc* denied. 4/16/13: Petition for writ of certiorari filed. 6/24/13: Petition for writ of certiorari denied.

			in the U.S. Supreme Court, which was denied on 6/24/13.	
Stored Communications Act ("SCA")	*Cousineau v. Microsoft Corp.*, No. C-11-1438 (W.D. Wash. 3/25/14)	Motion for Summary Judgment Granted	A federal judge in Washington held that Microsoft did not illegally access geolocation data stored in the plaintiff's smartphone's RAM through its camera application and Windows Mobile 7 operating system's location framework because the plaintiff consented to Microsoft's access by leaving the phone's master location switch on. The plaintiff alleged that Microsoft had violated the SCA by accessing geolocation data on her phone without permission by constructing the camera application to access the location data stored in the phone's RAM even though the plaintiff had refused the camera application's prompt to enable location services.	3/25/14: Motion for summary judgment granted.
Stored Communications Act ("SCA") Electronic Communications Privacy Act ("ECPA") Computer Fraud and Abuse Act ("CFAA")	*Dunstan v. comScore, Inc.*, No. 11-cv-5807 (N.D. Ill. 2/20/14)	Complaint Filed Class Certified Appeal of Class Certification Denied Motion for Partial Summary Judgment Filed	A federal judge in Illinois has approved the largest class of plaintiffs ever certified on an adversarial basis, in an action brought against online data research company comScore for alleged violations of the SCA, ECPA, and CFAA. According to the class complaint, comScore collects personal information from consumers' computers that it then sells to media outlets without the consumers' knowledge or consent. The certified class includes over one million individuals who have, since 2005, downloaded and installed comScore's tracking software onto their computers via one of comScore's third-party bundling partners. The Seventh Circuit summarily denied comScore's interlocutory petition to appeal the class certification. On 2/20/14, plaintiffs filed a motion for partial summary judgment on their CFAA, SCA, and ECPA claims; the substance of the motion was filed under seal.	8/23/11: Complaint filed. 10/25/12: Amended complaint filed. 4/2/13: Motion to certify class granted. 6/11/13: Appeal of class certification denied. 2/20/14: Motion for partial summary judgment filed.
Telephone Consumer Protection Act ("TCPA")	*Sherman v. Yahoo! Inc.*, No. 3:13-cv-0041 (S.D. Cal. 3/3/14)	Summary Judgment Denied	A federal judge has refused to grant summary judgment to Yahoo!, holding that sending a single unsolicited text message can give rise to a claim under the TCPA. On 3/3/14, Yahoo! filed a motion asking the court to reconsider its ruling on the grounds that the court had incorrectly relied upon the FCC 's definition of an Automatic Telephone Dialing System ("ATDS"), since the Ninth Circuit had previously ruled that the TCPA's ATDS definition was unambiguous and because Yahoo!'s text service should not qualify as an ATDS merely because software could be written to dial all of the numbers in its database. On 3/11/14, the court stayed the proceedings pending Yahoo!'s motion for reconsideration; the motion remains pending.	2/3/14: Motion for summary judgment denied. 3/3/14: Motion for reconsideration of summary judgment filed.

COURTS (continued)

Telephone Consumer Protection Act ("TCPA")	*Emanuel v. Los Angeles Lakers Inc.*, No. 13-55678 (9th Cir.12/31/13)	Notice of Settlement Filed	The Los Angeles Lakers have reached a settlement in a proposed class action suit in which the team was sued under the TCPA for sending infringing text messages. Plaintiff alleged that after he texted a message to be displayed in the Staples Center during a Lakers' game, he received two unsolicited texts from the Lakers, first in confirmation of his initial message and then in response to his request to stop sending further messages. A California federal district court judge dismissed the suit finding that, by sending his original text, the plaintiff agreed to receive confirmatory texts. The plaintiff appealed, arguing that the district court's dismissal should be reversed because the TCPA applies to any call placed with an auto-dialer and does not require that calls be placed in bulk to apply, and the plaintiff did not consent to receive automated text messages. The parties filed a notice of settlement on 12/31/13; the terms of the settlement have not yet been made public.	12/31/13: Notice of settlement filed.
Third-Party Doctrine	*Patel v. Los Angeles*, No. 08-56567 (9th Cir. 12/24/13)	Opinions Issued Petition for Rehearing *En Banc* Granted Oral Argument Held Opinion Issued	In *Patel*, the court rejected a facial Fourth Amendment challenge to a law that required hotel operators to maintain information about their guests for 90 days (including name and address; car make, model, and license plate number; room number; dates; rates; and method of payment) and provide it to law enforcement on request. On 2/13/13, the full Ninth Circuit granted Patel's motion for a rehearing *en banc*. On 12/24/13, the full court reversed the panel's decision and held that the law requiring hotel operators to provide guest records to law enforcement on request was facially invalid under the Fourth Amendment because it allows for inspection prior to judicial review and the inspection of guest records qualifies as a "search." The court held that the law must afford hotel operators the chance to challenge inspection requests in court before imposing penalties for non-compliance. Two dissenting opinions were also issued, each joined by three other judges. The first dissented on the ground that any search conducted pursuant to the law was invalid. The second dissented on the ground that the majority "ignored the facial nature of the plaintiff's challenge to the ordinance" and did not demonstrate that a search would be unreasonable.	7/17/12: Opinion issued. 2/13/13: Petition for rehearing *en banc* granted. 6/24/13: Oral argument held. 12/24/13: Opinion issued.
Video Privacy Protection Act ("VPPA")	*In re Netflix Privacy Litigation*, No. 5:11-cv-00379-EJD (N.D. Cal. 3/18/13) *Milans v. Netflix, Inc.*, No. 13-15754	Settlement Reached Notice of Appeal Filed	A settlement was reached in litigation relating to Netflix's alleged unlawful retention of video rental records under the VPPA and California state law. The parties entered private mediation on 12/2/11, and a settlement was reached 2/10/12 and preliminarily approved 7/5/12. The terms of the settlement require Netflix to decouple a subscriber's viewing history from his identification and payment information if the subscriber's service has been cancelled for one year or more. A number of objections to the proposed	12/1/11: Private mediation entered. 2/10/12: Settlement reached. 7/5/12: Preliminary approval of settlement.

	(9th Cir. 12/19/13)		settlement were filed by class members, but a motion for final approval of the settlement was filed by lead class counsel on 10/31/12. The court issued final approval of the settlement on 3/18/13 and dismissed the case. On 4/16/13, multiple objectors filed appeals in the Ninth Circuit. Opening briefs were filed by some objectors on 8/20/13, although objectors in one of the appealed cases failed to file a brief and that case was dismissed for lack of prosecution on 9/27/13. On 12/6/13, two of the appellants filed a motion for voluntary dismissal, which was granted by the court on 12/19/13. The case will proceed as to the other appellants.	3/18/13: Settlement approved; case dismissed. 4/16/13: Notice of appeal. 8/20/13: Opening briefs filed.
Video Privacy Protection Act ("VPPA")	*Locklear v. Dow Jones & Co.*, No. 1:14-cv-00744 (N.D. Ga. 3/13/14)	Complaint Filed	Users of the Roku set-top box have brought a proposed class action suit against The Wall Street Journal under the VPPA for disclosing user information without consent to third-party data analytics and advertising companies each time customers used the WSJ Channel on their Roku boxes to watch content.	3/13/14: Complaint filed.
Video Privacy Protection Act ("VPPA")	*In re Hulu Privacy Litigation*, No. 3:11-cv-03764-LB (N.D. Cal. 12/20/13)	Order Denying Motion to Dismiss Amended Complaint Filed Motion for Class Certification Filed Motion for Summary Judgment Filed Motion for Summary Judgment Denied	In denying a motion to dismiss a claim against Hulu for a violation of the VPPA, a district court rejected the defendant's argument that the VPPA does not apply to online streaming services. Although Hulu did not exist when the VPPA was passed, it is a "video tape service provider" within the meaning of the statute. The statute will reach any person engaged in the business of rental, sale, or delivery of prerecorded video cassette tapes or similar audiovisual materials. On 11/30/12, the plaintiff filed an amended complaint focusing solely on VPPA-related claims. Hulu filed an answer on 12/21/12 and discovery in the case has begun. Trial has been tentatively scheduled for July 2014. On 8/26/13, plaintiffs filed their motion for class certification, which remains pending. Hulu filed a motion for summary judgment on 10/1/13, arguing that plaintiffs have not established a legally cognizable injury. The court denied Hulu's motion on 12/20/13 because the language of the VPPA only requires a showing of wrongful disclosure, not actual injury, to recover damages.	7/29/11: Complaint filed. 3/30/12: Motion to dismiss filed. 6/11/12: Motion to dismiss granted as to all claims save VPPA. 8/10/12: Motion to dismiss denied as to VPPA. 11/30/12: Amended complaint filed. 12/21/12: Answer filed. 8/26/13: Motion for class certification filed. 10/1/13: Motion for summary judgment filed. 12/20/13: Motion for summary judgment denied.

COURTS (continued)

Video Privacy Protection Act ("VPPA")	*Mollett v. Netflix Inc.*, No. 5:11-cv-01629-EJD (N.D. Cal., 8/17/12) *Mollett v. Netflix Inc.*, No. 12-17045 (9th Cir. 4/8/13)	Order Granting Motion to Dismiss Appeal Filed Appellate Briefs Filed	Plaintiff's lawsuit alleged violations of the VPPA when Netflix displayed a user's viewing history on his TV screen when accessed using a Netflix-capable device. The court dismissed the complaint, holding that it was impossible for Netflix to know who was watching, and plaintiffs could restrict access to the data. The plaintiff has filed an appeal with the Ninth Circuit. Briefs have been filed; no date has been set for oral argument.	8/17/12: Case dismissed with prejudice. 9/13/12: Notice of appeal filed. 12/21/12: Appellant's opening brief filed. 2/22/13: Opposition brief filed. 4/8/13: Reply brief filed.
Video Privacy Protection Act ("VPPA") Wiretap Act	*In re Nickelodeon Consumer Privacy Litigation*, No. 12-cv-07829 (D.N.J. 1/15/14)	Complaints Filed Cases Consolidated	Six similar class action complaints were filed on 12/21/12 against Viacom and Google alleging violations of the Wiretap Act and VPPA, as well as asserting various state law claims. Each suit proposes a class of users under the age of 13, but notably none of the complaints allege a violation of the Children's Online Privacy Protection Act ("COPPA"), which generally prohibits the intentional online collection of personal information of children under the age of 13. The complaints allege that Viacom, which operates various websites targeted toward children, unlawfully tracks the Internet communications and video viewing habits of users of those sites. Google's alleged involvement comes from its ownership of the doubleclick.net ad network, which placed cookies on the computers of the child users. The actions have been consolidated in the District of New Jersey. An amended consolidated complaint was filed on 10/23/13. Viacom filed a motion to dismiss the amended complaint on 1/15/14 on the grounds that plaintiffs lack standing because they have not alleged an injury-in-fact and because they failed to state a claim under the VPPA and ECPA.	12/21/12: Complaints filed. Jan. – Feb. 2013: Cases stayed pending consolidation order. June 2013: Cases consolidated. 10/23/13: Amended consolidated complaint filed. 1/15/14: Motion to dismiss filed.
Wiretap Act	*In re Google Inc. Street View Electronic Comm'cns Litig.*, No. 3:10-md-02184-JW (N.D. Cal. 7/18/11) *Joffe v. Google Inc.*, No. 11-17483 (9th Cir. 12/27/13)	Motion for Certificate of Appealability Granted Appellate Briefs Filed Oral Argument Held Opinion Issued	Google has appealed a partial denial of its motion to dismiss litigation relating to its admission that it captured data from unsecured wireless networks as part of its Street View program. Google argued that the Wiretap Act permits interception of "readily accessible" radio transmissions, and that the networks at issue were not password-protected. The district court disagreed, stating that the data could not have been captured without sophisticated technology. Opening, answering, and reply briefs have been filed before the Ninth Circuit on 2/8/12, 3/26/12, and 4/23/12, respectively. EPIC also filed an amicus brief on 4/6/12. Oral argument was	11/8/10: Consolidated class action complaint filed. 12/7/10: Motion to dismiss filed. 6/29/11: Motion to dismiss granted in part and denied in part.

		Amended Opinion Issued	held on the interlocutory appeal 6/10/13. On 9/10/13, the Ninth Circuit affirmed, holding that data transmitted over a Wi-Fi network is not a "radio communication" that is "readily accessible to the general public" under the Wiretap Act, and is therefore not exempt under the law. Additionally, the court further held that, regardless of whether the data transmission is a "radio communication," it is still not "readily accessible to the general public" under the plain meaning of that phrase. Google has filed a petition for rehearing *en banc*. On 12/27/13, the court denied Google's petition for rehearing *en banc* but issued an amended opinion. The panel opinion held that because "radio communication" excludes payload data transmitted over a Wi-Fi network, the public accessibility requirement in § 2510(16) is inapplicable to the "electronic communication" exception under § 2511(2)(g)(1). On 2/7/2014, the district court lifted a stay of the case and ordered discovery to proceed.	7/18/11: Motion for certificate of appealability granted. 4/23/12: Appellate briefs filed. 6/10/13: Oral argument held. 9/10/13: Opinion issued. 12/27/13: *En banc* rehearing denied, but opinion amended.
Wiretap Act	*In re Facebook Internet Tracking Litig.*, No. 5:12-md-02314 (N.D. Cal. 7/2/12)	Complaint Filed Motion to Dismiss Filed	Eleven lawsuits against Facebook alleging that the company unlawfully tracks users after they have logged out of their accounts have been consolidated before a California district court. The class plaintiffs filed their first amended class action complaint on 4/3/12. The complaint alleges that Facebook intentionally intercepted information without the consent of its members and did so in violation of its Privacy Policy, and also caused other sites using Facebook technology (such as washingtonpost.com) to violate their privacy policies. The complaint also alleged tort claims including unjust enrichment, intrusion upon seclusion, and trespass. Facebook has filed a motion to dismiss, which remains pending before the court as of April 2014.	4/3/12: Complaint filed. 7/2/12: Motion to dismiss filed.
Wiretap Act Stored Communications Act ("SCA") Computer Fraud and Abuse Act ("CFAA")	*In re Google, Inc. Privacy Policy Litigation*, No. 12-cv-01382 (N.D. Cal. 1/16/14)	Complaints Filed (*De Mars*, *Nisenbaum*) Motion to Dismiss Granted Amended Class Complaint Filed Motion to Dismiss Granted Second Amended Class Complaint	Following Google's change to a new unified privacy policy, from 8/19/04 to 2/29/12, various class action lawsuits were filed against the company by consumers in California and New York on behalf of Google account users and Android device owners, , who continued to use the Google accounts or devices after the new privacy policy came into effect on 3/1/12. The cases were consolidated in the Northern District of California. The consolidated complaint asserted violations of the Wiretap Act (for interception and aggregation of data for Google's financial benefit), the SCA (both for exceeding authorized access to data stored on Google systems and for placing cookies on users' computers), and the CFAA (for unauthorized access to email and search histories), as well as state law. On 12/28/12, the court granted Google's motion to dismiss the complaints with leave to file	3/20/12: Complaints filed. 6/8/12: Consolidated class action complaint filed. 8/6/12: Motion to dismiss filed. 12/28/12: Motion to dismiss granted. 3/7/13: Amended complaint filed.

		Filed	a consolidated amended complaint. In dismissing the case, the court ruled that the plaintiffs had failed to demonstrate injury sufficient to confer standing. On 3/7/13, plaintiffs filed an amended complaint, asserting various harms suffered as a result of Google's new privacy policy, including: (1) misappropriation of name or likeness; (2) cost incurred to replace Android devices following the policy change; (3) the incremental amount of electricity and bandwidth needed to involuntarily submit information pursuant to the new policy; (4) invasion of privacy interests; (5) Google's unauthorized access and disclosure of private communications; and (6) Google's unauthorized interception of those communications. Google filed a motion to dismiss the amended complaint on 5/14/13. The court granted the motion leave to amend on 12/3/13, explaining that although plaintiffs had alleged injuries sufficient to establish standing, their claims still failed to meet the pleading requirements. Plaintiffs filed a second amended complaint on 1/16/14. Google filed a motion to dismiss the amended complaint on 2/21/14, arguing that the second amended complaint fails for similar reasons as the previous complaints. See the "International Developments Affecting U.S. Businesses" section below for additional information on the international reaction to the new Google privacy policy.	5/14/13: Motion to dismiss filed. 12/3/13: Motion to dismiss granted. 1/16/14: Amended complaint filed. 2/21/14: Motion to dismiss amended complaint filed.

INDUSTRY DEVELOPMENTS

Topic / KeyWords	Group Name(s)	Action	Description	Status / Comments
Cybersecurity	Securities Industry and Financial Markets Association ("SIFMA")	Report on Cyberattack Simulation Released	On 7/18/13, SIFMA orchestrated simulated cyberattacks intended to disrupt trading on U.S. equities markets to test the effectiveness of existing cybersecurity measures. The exercise, named Quantum Dawn 2, followed a 2011 simulation named Quantum Dawn. More than twice as many entities participated. On 10/21/13, Deloitte & Touche LLP released a report analyzing the simulation.	7/18/13: Cyberattack simulation held. 10/21/13: Report on cyberattack simulation released.
Cybersecurity	TRUSTe	Certification Announced	On 11/18/13, TRUSTe certified Merck & Co. as the first health-care company and second multinational company to become certified under the Asia-Pacific Economic Cooperation Cross Border Privacy Rules (CBPR). TRUSTe is the first accountability agent under the system, which is intended to protect the privacy of consumer data moving between the U.S. and APEC member economies by requiring companies to develop their own internal business rules on cross-border privacy procedures.	11/18/13: Certification announced.
Data Breach	CorporateCarOnline.com	Data Breach Reported	On 11/4/13, a St. Louis-based provider of online management services for limousine companies experienced a data breach that exposed the personal and financial information of hundreds of thousands of customers from approximately 500 limousine and car services around the country, including celebrities such as Tom Hanks and lawmakers such as Rep. John Conyers. The database was in plain-text format and therefore easily readable.	11/4/13: Data breach reported.
Data Breach	JP Morgan	Data Breach Reported	A cyberattack exposed as many as 465,000 JP Morgan accounts across the U.S. between July and September. On 12/3/13, JP Morgan reported the cyberattack to Connecticut Treasurer Denise L. Nappier, who reported that she was "dismayed" at the two-and-a-half month delay between the breach and notification.	12/3/13: Data breach reported.
Data Breach	Target	Data Breach Reported	On 12/19/13, Target announced that it experienced a data breach compromising the data of approximately 40 million customers who used credit or debit cards at its store in November and December. The compromise included customer names as well as payment card information, including encrypted PIN data for customers' debit cards. In addition, the names, mailing addresses, and phone numbers or e-mail addresses for up to 30 million additional customers were stolen. Target issued a statement	12/19/13: Data breach reported. 3/5/14: Resignation of CIO announced.

			that customers would have no liability for the cost of any fraudulent charges arising from the breach. On 2/4/14, Target apologized to Congress for the breach. On 3/5/14, Target announced the resignation of its Chief Information Officer Beth Jacob.	
Data Breach	Snapchat	Data Breach Reported	On 12/31/14, Snapchat, a service that allows users to share ephemeral photos and videos, experienced a breach when attackers released a database of 4.6 million usernames and phone numbers. Snapchat had been informed of vulnerabilities in the app in August 2013 by Gibson Security.	12/31/13: Data breach reported.
Data Breach	Neiman Marcus	Data Breach Reported	On 1/22/14, Neiman Marcus reported that it faced a malware attack from 7/16/13 to 10/30/13, which affected payment card data of approximately 1.1 million customers. Credit card issuers have notified the company that approximately 2,400 payment cards were used fraudulently since the breach. The hackers set off alerts on the company's security systems about 60,000 times during the breach but remained undetected by the company.	1/22/14: Data breach reported.
Data Privacy Children's Online Privacy	Center for Digital Democracy	Investigations Requested	On 12/18/13, the Center for Digital Democracy ("CDD") requested that the FTC investigate the website Marvelkids.com and a Hello Kitty mobile application for failure to comply with the notice and parental consent requirements of COPPA.	12/18/13: Investigations requested.
Data Privacy Data Security	EPIC ACLU Various Consumer Advocacy Groups	Letter Sent to White House	On 2/10/14, various consumer advocacy groups sent a letter to the White House, urging it to include a public comment process in its recently launched review of privacy concerns related to big data. The letter requested that John Holdren, director of the Office of Science and Technology Policy at the White House, issue a request for information on several issues such as the adequacy of legal frameworks governing big data.	2/10/14: Letter sent.
Data Privacy Data Security	Retail Industry Leaders Association Financial Services Roundtable	Partnership Announced	On 2/13/14, the Retail Industry Leaders Association, Financial Services Roundtable, and several other trade associations announced a partnership to share information and to fight fraud. Industry groups stated that the partnership will focus on exploring approaches to increased information sharing and better payment card security technology, as well as discussing areas of disagreement between banks and merchants.	2/13/14: Partnership announced.

INDUSTRY DEVELOPMENTS (continued)

Data Privacy Data Security Children's Online Privacy Mobile Apps Mobile Devices Online Behavioral Advertising	Direct Marketing Association	Guidelines Released	On 2/18/14, the Direct Marketing Association released new guidelines for ethical business practices. These self-regulatory guidelines guide data-driven marketers' best practices and advocate for strong protection of consumer information. They include updated provisions addressing children's privacy and COPPA, health information and HIPAA, compliance with the TCPA, and providing notice and choice for mobile applications.	2/18/14: Guidelines released.
Data Privacy Data Security	EPIC and various public interest groups	Letter Sent to White House	On 2/24/14, a coalition of public interest groups issued a letter to President Obama asking to revive a stalled push for congressional action on a "Consumer Privacy Bill of Rights," which the White House called on Congress to pass in February 2012. The proposal has gained little ground thus far.	2/24/14: Letter sent.
Data Privacy Data Security	EPIC Center for Digital Democracy	Request for Investigation Sent to FTC	On 3/6/14, EPIC and the Center for Digital Democracy filed a request for investigation with the FTC, stating that WhatsApp's status as a pro-privacy mobile application would end after its acquisition by Facebook, which will mine user data. The request stated that WhatsApp failed to adequately warn its users that its privacy promises may change as a result of the acquisition. WhatsApp's CEO stated in a 3/17/14 blog post that it is still committed to user privacy.	3/6/14: Request for investigation sent.
Data Privacy Data Security	Visa Mastercard	Cross-Industry Group Announced	On 3/7/14, Visa and Mastercard announced the formation of a cross-industry group focused on the adoption of EMV chip technology, which generates a unique code for every transaction, in the U.S. The group will include banks of all sizes, credit unions, acquirers, retailers, point-of-sale device manufacturers and industry trade groups.	3/7/14: Cross-industry group announced.
Data Privacy ECPA	Google	Transparency Report Released	On 1/27/14, the DOJ announced a deal with Google, Microsoft, Yahoo, Facebook, and LinkedIn allowing these companies to release more information about the volume of user data the U.S. government demands they provide. The terms of the deal prevent the companies from itemizing the collection beyond bands of thousands of data requests served on them under the Foreign Intelligence Surveillance Act ("FISA"). The companies are	1/23/13: Google Transparency Report released. 1/28/13: News reports indicate that Google is talking to various advocacy

			also required to delay by six months disclosing information about requests. Google received FISA court requests for the metadata of up to 999 customer accounts, and the content of communications from between 9,000 and 9,999 customers between January and June of 2013. On 2/3/14, Google's legal director for law enforcement and information stated in a blog post that Google still believes that more transparency is needed so that the public can understand surveillance laws.	groups about a joint lobbying effort to amend ECPA. 1/27/14: Google and other tech and communication companies reach deal with DOJ. 2/3/14: Google FISA transparency report released.
Data Privacy ECPA	Microsoft	Transparency Report Released	On 2/3/14, Microsoft released its FISA Transparency Report. During the first six months of 2013, Microsoft received FISA court orders for communications content related to between 15,000 and 15,999 "accounts or individual identifiers."	2/3/14: FISA transparency report released.
Data Privacy ECPA	Yahoo	Transparency Report Released	On 2/3/14, Yahoo released its FISA Transparency Report. Yahoo disclosed that it received FISA requests for communications content from between 30,000 and 30,999 accounts over the first six months of 2013, and up to 999 customer accounts were subject to FISA court orders for metadata.	2/3/14: FISA transparency report released.
Data Privacy ECPA	Facebook	Transparency Report Released	On 2/3/14, Facebook released its FISA Transparency Report. Facebook disclosed that during the first half of 2013, it received FISA court orders for content data from between 5000 and 5,999 accounts, a rise of about 1,000 from the previous six month period, and customer metadata associated with up to 999 accounts.	2/3/14: FISA transparency report released.
Data Privacy ECPA	LinkedIn	Transparency Report Released	On 2/3/14, LinkedIn released its FISA Transparency Report. LinkedIn disclosed that during the first six months of 2013, it received less than 250 national security requests, including national security letters and other requests, relating to less than 250 accounts.	2/3/14: FISA transparency report released.
Data Privacy ECPA	Verizon	Transparency Report Released	On 2/18/14, Verizon released its FISA Transparency Report. Verizon released a transparency report showing that it received a total of 271,545 subpoenas, warrants, and orders from law enforcement for customer data in 2013. Verizon received less than 1,000 FISA requests for content in the first half of 2013, affecting 4,000 and 4,999 "customer selectors" used to identify a Verizon customer.	2/18/14: FISA transparency report released.

INDUSTRY DEVELOPMENTS (continued)

Data Privacy ECPA	AT&T	Transparency Report Released	On 3/3/14, AT&T released its FISA Transparency Report. AT&T published a transparency report showing that it received 301,816 subpoenas, warrants, and orders for customer data in 2013. It received less than 1,000 FISA requests for content affecting 35,000 to 35,999 customer accounts in the first half of 2013.	3/3/14: FISA transparency report released.
Health Data Privacy and Security	European Federation of Pharmaceutical Industries Associations and Pharmaceutical Research and Manufacturers of America	Joint Principles Released	The European Federation of Pharmaceutical Industries and Associations and the Pharmaceutical Research and Manufacturers of America adopted principles for the sharing of clinical trial data. Researchers in Europe and the United States can request clinical trial study protocols and patient-level information on treatments under these principles, which contain requirements that researchers who obtain clinical trial data must publish their findings and companies must work with regulators to provide summaries of clinical trial results to patients who participate.	1/1/14: Joint principles take effect.
Health Data Privacy and Security	Ponemon Institute	Report Released	On 3/12/14, the Ponemon Institute released a report stating that the number of health-care breaches declined in 2013, but health-care industry concern about unauthorized access to personal information is on the rise. The report states that 75 percent of health-care organizations cite employee negligence as their greatest security concern.	3/12/14: Report released.
Mobile Apps Mobile Devices Data Security	PCI Security Standards Council	New Standards Released	On 11/7/13, PCI Security Standards Council released new versions of two of its data security standards, the Payment Card Industry Data Security Standard ("PCI DSS") and the Payment Application-Data Security Standard ("PA-DSS"). PCI DSS requires companies handling card transactions to maintain data security measures, face fines, or cut off the ability to process cards. PA-DSS assists software vendors in the development of secure payment applications. The updates to the PCI DSS focus on security risks resulting from third-party vendors and malware, botnets, and viruses. The new versions took effect 1/1/14, but the previous versions will remain active until 12/31/14 to provide companies time to adapt to the changes.	8/15/13: New standards announced. 11/7/13: Release date of new standards. 1/1/14: Effective date of new standards.
Mobile Devices	Future of Privacy Forum	Code of Conduct Released	On 10/22/13, the Future of Privacy Forum released a code of conduct called the "Mobile Location Analytics Code of Conduct" that calls for U.S. retailers to inform consumers of in-store tracking and to provide opt-out instructions on signage in the stores.	10/22/13: Code of conduct released.

INDUSTRY DEVELOPMENTS (continued)

Online Behavioral Advertising	World Wide Web Consortium ("W3C") Digital Advertising Alliance ("DAA")	Working Draft Released Consensus Action Document Released New Draft Released Alternative Draft Released Co-Chairs Reach Decision Two New Co-Chairs Appointed Draft of Technical Specifications Released	On 9/9/11, W3C, the standards body that develops the protocols and guidelines for the Internet, announced a new project to standardize the Do-Not-Track opt-out tools already a part of Firefox, Internet Explorer, and Safari. The project, called the Tracking Protection Working Group, will bring together browser makers, advertisers, and developers to standardize a simple way for web browsers to opt out of online tracking. On 11/14/11, W3C released the first draft of its proposed standards for implementing Do-Not-Track online. The final standard was supposed to be released in the summer of 2012; however, talks convened by W3C have appeared to reach a stalemate. Privacy advocates and industry representatives are now lobbying the FTC and lawmakers to intervene and help settle differences. On 10/2/12, the Digital Advertising Alliance ("DAA") sent an open letter to W3C arguing that W3C should not be in charge of setting privacy standards. Consumer Watchdog sent a letter to FTC Chairman John Leibowitz on 1/30/13 arguing that the self-regulatory efforts through the W3C were "virtually dead in the water." The group called on the FTC to push Congress to pass Do-Not-Track legislation. On 4/30/13, W3C's Tracking Protection Working Group released a working draft for standardizing Do-Not-Track preferences in web browsers. On 5/6-8/13, the Tracking Protection Working Group held its eighth face-to-face meeting. Following the meeting, the Working Group released a consensus action document. On 6/14/13, the Tracking Protection Working Group released a draft as it quickly approached the July 2013 last call deadline. The draft was based on the "Consensus Action Summary" the group achieved at its face-to-face meeting in May. In the draft, the default setting for do-not-track preference is "unset." On 6/26/13, the Direct Advertising Alliance ("DAA") released an alternative draft. The alternative draft defines tracking in terms of a user's browsing activity and would allow marketers to use "aggregate scoring," where marketers build a user profile without URL browsing history being attached. On 7/15/2013, the co-chairs of the Tracking Protection Working Group decided to use the June Draft provided by the Working Group as the base text to push toward the "Last Call" deadline for feedback. The co-chairs noted that Apple, Microsoft, and Mozilla all supported the June Draft. Following the Working Group's July meeting, several important members resigned. On 7/30/13, Jonathan Mayer of the Stanford Center for Internet	9/9/11: W3C Tracking Protection Working Group announced. 11/14/11: Draft proposed Do-Not-Track standard released. 10/2/12: Open letter from the DAA. 1/30/13: Consumer Watchdog Letter to FTC Chairman. 4/30/13: Working draft released. 5/6-8/13: Face-to-face meeting held. 5/13/13: Consensus action document released. 6/14/13: Draft released. 6/19/13: Conference call held. 6/26/13: Alternative draft released. 7/15/13: Co-chairs decision released. 9/18/13: Two co-chairs appointed. 1/15/14: Draft of technical specification released.

			and Society resigned because the group failed to meet its July "Last Call" deadline. On 8/28/13, co-chair Peter Swire resigned to join a new intelligence review panel within the Executive Branch. On 9/17/13, DAA withdrew from future participation in the Working Group. DAA stated that after two years of participation, it no longer believed the Working Group was capable of fostering a workable "Do Not Track" solution. W3C noted that many of DAA's members remained involved in the Working Group. On 9/18/13, W3C announced that it appointed two new co-chairs to the Working Group: Justin Brookman from the Center for Democracy & Technology and Carl Cargill from Adobe Systems, Inc. W3C also announced plans to release DNT 1.0 sometime in 2013 or 2014. On 1/15/14, the group released the latest draft of the technical specification, the "tracking preference expression" (TPE), which describes the elements of the DNT header.	
Online Behavioral Advertising Data Privacy Mobile Apps Mobile Devices	Network Advertising Initiative ("NAI") DAA	Annual Compliance Report Released Update to Code Announced Draft Revised Code of Conduct Released Final Code of Conduct Released Mobile Application Code Released Application of Self-Regulatory Principles to Mobile Environment Released	On 3/1/13, NAI released a draft of its revised code of conduct for Online Behavioral Advertising ("OBA"). The draft would require companies delivering targeted advertising in the online space to provide enhanced notice regarding their data collection and use practices in and around the targeted ads served. The revised code of conduct modified the definition of personally identifiable information to exclude data used or intended to be used to determine the precise location of an individual. The revised code of conduct also removed geolocation information from its definition of sensitive data, but maintains the requirement of opt-in consent to collect geolocation information. Other revisions include: (1) adding sexual orientation as a category of sensitive data; (2) changing the name of online behavioral advertising to interest-based advertising; (3) requiring disclosure of the technologies used for interest-based advertising; and (4) prohibiting the use of data collected through interest-based advertising for certain eligibility decisions, like employment, health care, and insurance eligibility. The revised code of conduct clarified what it means to honor a user's opt-out. The revised code of conduct would allow its members to continue to collect data for internal operations even after a user opts out. NAI accepted comments on the draft revision until 4/5/13.	3/1/13: Draft revised code of conduct released. 5/16/13: Final code of conduct released. 5/16/13: NAI's compliance and enforcement procedures released. 7/24/13: NAI released Mobile Application Code. 7/24/13: DAA released its Mobile Application Principles.

			On 5/16/13, NAI released its final revised code of conduct. The final code of conduct made no significant substantive changes to the draft code of conduct released in March. NAI stated it would begin enforcing the revised code of conduct in 2014. In conjunction with the release of the final code of conduct, NAI also released a document titled "NAI Compliance and Enforcement Procedures" to compile NAI's compliance and enforcement procedures into one document. On 7/24/13, NAI released its "Mobile Application Code," which is substantially based on its interest-based advertising code of conduct. In addition, DAA released its "Application of Self-Regulatory Principles to the Mobile Environment" as an update to its online behavioral advertising principles relating to the mobile space. Generally, these principles require transparency in data collection, provide consumers with control over collection and use of their data, provide appropriate security for collected data, and require consent to material changes in the way data are handled.	
Online Behavioral Advertising	Online Interest-Based Advertising Accountability Program	Decisions Released	The Online Interest-Based Advertising Accountability Program reminded five companies, including BMW, Scottrade, and 23andMe, of their obligations to provide notice and choice when consumer information is collected for online behavioral advertising. The program is operated by the Council of Better Business Bureaus Advertising Self-Regulatory Council and is an accountability agent responsible for enforcing the Self-Regulatory Principles for Online Behavioral Advertising.	11/18/13: BMW decision. 11/18/13: Scottrade decision. 11/20/13: 23andMe decision.

INTERNATIONAL DEVELOPMENTS AFFECTING U.S. BUSINESSES

Topic / Key Words	Group Name(s)	Action	Description	Status / Comments
International Privacy Protection Online Behavioral Advertising User Tracking Breach Notification	Council of the European Union	Revised EU e-Privacy Directive (2002/58/EC) as amended by (2009/136/EC)	In late June 2013, the European Commission issued a Regulation that provided specific notification measures to be taken in all member states following a breach of personal data held by publicly available communication services. As a Regulation, the rules apply directly to all member states and do not require implementation. The new rules apply to providers of "publicly available electronic communications services," which includes telecommunications operators and internet service providers, and generally require these providers to make detailed notifications to national data protection authorities of breaches within 24 hours in a standardized format to be used across all member states. If necessary, providers may make an initial report within 24 hours and provide detailed follow-up within three days; delays beyond three days must be supported by a "reasoned justification," but there has been no guidance yet on what would suffice for such a justification. The Regulation went into effect on 8/25/13.	8/25/13: Breach notification Regulation goes into effect.
International Privacy Protection Cross-Border Transfers	Asia-Pacific Economic Cooperation ("APEC")	Transfer Declaration Signed	On 11/13/11, APEC leaders signed a declaration pledging to implement the new Cross Border Privacy Rules System. Under the rules, companies adopt and agree to abide by internal privacy rules coupled with third-party oversight. The declaration stated that the signors would implement information and communication technology policies related to data privacy and security that would minimize differences in the area across the various countries. On 5/22/12, the United States sent a formal letter indicating it wishes to be a participant in the program. The United States was approved on 7/25/12, and the FTC has become the first enforcement authority in the system. See "Federal Agencies" section above for more details. On 1/16/13, Mexico entered as the second participant in the program. On 6/7/13, Japan filed a formal application to become the third member of the program. The program took another step forward when TRUSTe was approved as the first "accountability agent" authorized to examine and approve data transfer applications between member states.	7/25/12: U.S. approved as a participant. 1/16/13: Mexico approved as a participant. 6/7/13: Japan files application to join. 6/25/13: TRUSTe approved as first accountability agent.

International Privacy Protection Cross-Border Transfers U.S.-EU Safe Harbor	European Parliament	Report Issued Resolution Passed	A report commissioned by the European Parliament and authored by Microsoft's former chief privacy officer, Caspar Bowden, strongly criticized the Safe Harbor program as being completely ineffective at safeguarding European citizens' data from American authorities. The Bowden report recommended encouraging the development of EU-based cloud computing capacity and the reinstatement of a previously deleted principle in the proposed Data Protection Regulation that would require prior approval of a data protection authority before personal data stored in Europe may be accessed by entities in other countries. In response to the Bowden report, the European Parliament released its own draft report and resolution containing steps to protect individuals against state surveillance of their personal data. The establishment of the proposed "European digital habeas corpus" would result in the suspension of data transfer programs between the EU and the U.S., such as the U.S.-EU Safe Harbor Program and the U.S.-Europe Transatlantic Trade and Investment Partnership (TTIP). On 2/12/14, lawmakers on the key Civil Liberties, Justice, and Home Affairs ("LIBE") Committee approved the nonbinding resolution by a vote of 33-7. On 3/12/14, the full European Parliament passed the resolution.	12/23/13: Draft report and resolution released. 2/12/14: LIBE lawmakers approves resolution. 3/12/14: European Parliament approves resolution.
International Privacy Protection Cross-Border Transfers U.S.-EU Safe Harbor	Luxembourg National Data Protection Commission (CNDP)	Complaints Dismissed	The Luxembourg National Data Protection Commission dismissed complaints by an Austria-based student group against Microsoft and its Skype online service that stated that the companies could not provide their EU users with an "adequate level of protection" of personal data, as required under the EU Data Protection Directive, because the personal data they processed could end up in the hands of U.S. surveillance officials. The CNDP reasoned that the companies are included in the U.S.-EU Safe Harbor program to allow transfer of the personal data of EU citizens to countries outside the EU, and have provided the CNDP with formal assurances that they processed data in accordance with the U.S.-EU Safe Harbor program.	11/15/13: Complaints dismissed.
International Privacy Protection	Asia-Pacific Economic Cooperation ("APEC")	Transfer Declaration Signed	On 11/13/11, APEC leaders signed a declaration pledging to implement the new Cross Border Privacy Rules (CBPR) System. Under the rules, companies adopt and agree to abide by internal privacy	7/25/12: U.S. approved as a participant.

Cross-Border Transfers			rules coupled with third-party oversight. The declaration stated that the signers would implement information and communication technology policies related to data privacy and security that would minimize differences in the area across the various countries. On 5/22/12, the United States sent a formal letter indicating it wishes to be a participant in the program. The United States was approved on 7/25/12, and the FTC has become the first enforcement authority in the system. **See "Federal Agencies" section above for more details.** On 1/16/13, Mexico entered as the second participant in the program. On 6/7/13, Japan filed a formal application to become the third member of the program. The program took another step forward when TRUSTe was approved as the first "accountability agent" authorized to examine and approve data transfer applications between member states. TRUSTe has certified a limited number of companies as being in compliance with APEC's CBPR, including IBM, Merck & Co., Lynda.com, and Yodlee. A CBPR website is now operational and lists accountability agents and certified companies.	1/16/13: Mexico approved as a participant. 6/7/13: Japan files application to join. 6/25/13: TRUSTe approved as first accountability agent.
International Privacy Protection Cross-Border Transfers	European Parliament	Resolution Passed	Citing alleged surveillance by U.S. agencies of EU citizens' data, the European Parliament passed a nonbinding resolution calling for the suspension of data-sharing under the U.S.-EU Terrorist Finance Tracking Program (TFTP). The resolution states that TFTP does not have sufficient data protection safeguards.	10/23/13: Resolution passed.
International Privacy Protection Cross-Border Transfers	APEC Art. 29 Working Party	Interoperability Map Released	The APEC and the EC's Article 29 Working Party released a data transfer interoperability map aimed at helping companies navigate the two blocs' cross-border data transfer mechanisms. The informal guidance sets out specific recommendations for structuring privacy practices in a manner that is compliant with both APEC and EU privacy requirements.	3/6/14: Map released.
International Privacy Protection Data Breach	European Commission European Parliament	Revised EU Data Protection Regulation	On 1/25/12, the European Commission released its proposed data protection Regulation. Unlike the prior Directive, which each member state transposed into its national laws with some flexibility, the Regulation would apply, as written, across all member states. The core provisions include: (1) a more expansive definition of "personal data"; (2) a "right to be forgotten" that will allow consumers to	1/25/12: Proposal released. 1/10/13: EU Parliament's draft report ("Albrecht Report") released.

			remove their data from websites if there are "no legitimate grounds" for it to be kept; (3) an explicit consent requirement; (4) a data protection agency in each country, responsible for the companies with headquarters in that country and for coordinating regulation of multinational companies; (5) an easier ability to access exported data from websites; (6) a requirement for data protection officers at companies with greater than 250 employees; (7) a requirement for data breach reporting within 24 hours of discovery; and (8) fines of up to 2% of global annual turnover. The draft Regulation has been subject to review, comments, and criticisms by a wide variety of parties, including committees of the EU Parliament and EU Council of Ministers (which must jointly approve the proposed regulation), representatives and committees of EU member states, representatives and committees of foreign nations, and other public and private actors. Various EU parliamentary committees submitted a total of over 3,000 draft amendments, many of which have been criticized as being overly favorable to business interests and potentially weakening the Regulation's ability to protect individual rights. The LIBE debated the amendments for months, repeatedly extending a vote originally scheduled for May 2013. On 10/21/13, LIBE voted to adopt a small fraction of the proposed amendments – less than 100 – and begin trilogue meetings with the Council of Europe and the European Commission. Notable amendments that were adopted included increasing maximum fines to €100 million or 5% of a company's global annual turnover (whichever is larger) and barring companies from turning over personal data in response to another country's subpoenas or court orders unless (1) with prior approval from regulators or (2) pursuant to a valid agreement for such transfers. The latter amendment was made in direct response to revelations of NSA surveillance of Europeans and may prove to be the most controversial as negotiations continue. At a summit in October 2013, European heads of state and government committed to a "timely" adoption of the new data protection legislation. On 3/4/14, the EU Council of Ministers discussed the data protection reform, focusing on its territorial scope and on aspects relating to	2/20/13: ITRE amendments proposed. 5/31/13: CNIL announces public inquiry into "right to be forgotten." 6/19/13: LIBE announces delay of final vote to either the Sept. or Oct. 2013 meeting. 10/21/13: LIBE approves nearly 100 amendments and initiates Council and Commission negotiations. 3/12/14: European Parliament approves amended Regulation

			international transfers. They supported the principle that non-European companies, when offering goods and services to European customers, will have to apply the EU data protection law in full. On 3/12/14, the European Parliament voted 621-10 with 22 abstentions in favor of adopting the amended form. This means the position of the Parliament is set in stone and will not change even if the composition of the Parliament changes following the European elections in May. This vote sets out the European Parliament's position on the draft regulation ahead of eventual negotiations on a final text with the EU Council. The next meeting of the EU Council of Ministers on the data protection reform will take place in June 2014.	
International Privacy Protection Data Breach	European Commission European Parliament	Proposed EU Cybersecurity Directive	On 2/7/13, EC Vice President Neelie Kroes proposed a new Cybersecurity Directive, called the EU Network and Information Security Directive. The stated purpose of the directive is to improve the security of the Internet, private networks, and critical information systems. The directive requires that member states require operators of public systems, critical infrastructures (*e.g.*, energy and transport systems), and key providers of information services to take steps to manage security risks and report serious incidents to national authorities. • **Scope**: The law applies to energy companies, air/maritime/rail/port companies, banks, stock exchanges, and the health care sector (including hospitals and private clinics). Software developers, hardware manufacturers, and public institutions are excluded. • **Breach Notification**: The breach notification provision is written vaguely, allowing for significant interpretation by member states. It requires that covered entities "notify to the competent authority incidents having a significant impact on the security of the core services they provide." It allows, but does not require, member states to inform the public (or to require that the entity inform the public). The breach notification provision differs from that which is proposed in the draft data protection regulation (above), in that no breach of personal information is required prior to notification. • **Security and Audits**: The directive gives national authorities the	7/23/12: Consultation opened. 2/7/13: Proposed directive released. 6/14/13: EDPS opinion issued. 7/4/13: ICO comments published. 3/13/14: European Parliament approves revised version.

			power to require covered entities to "provide information needed to assess the security of their networks" and to "undergo a security audit . . . and make the results thereof available" to authorities. On 3/13/14, the European Parliament voted to approve a revised version of the directive.	
International Privacy Protection Industrial Espionage	European Commission	Proposed EU Trade Secrets Directive	On 11/28/13, the European Commission issued a proposed directive to crack down on industrial espionage by calling for a uniform set of EU rules to be applied in the member states that incorporate a common definition of confidential business information, as well as procedures that will allow victims of stolen trade secrets to seek compensation.	11/28/13: Directive proposed.
International Privacy Protection Privacy Policies	Article 29 Working Party French Data Protection Authority ("CNIL") Spanish Data Protection Authority ("AEPD")	Letter Issued Coordinated Enforcement Actions Announced Fines Levied	Google has faced ongoing scrutiny from EU regulators regarding its privacy compliance practices. Google has repeatedly maintained that its Privacy Policy complies with EU data protection law and expressed its willingness to work with authorities. However, on 12/7/12, *The New York Times* reported that, during a two-day closed-door meeting, WP29 mapped out a strategy for enforcement actions against Google that could include individual actions in countries such as Ireland, Belgium, and Finland, where Google operates data centers. On 6/20/13, CNIL and the data protection authorities from France, Germany, Italy, the Netherlands, Spain, and the U.K. respectively launched enforcement actions against Google. Having already completed its investigation, CNIL gave Google three months to comply with French data protection law or face sanctions. On 9/27/13, CNIL announced that it would "designate a rapporteur for the purpose of initiating a formal procedure for imposing sanctions." The CNIL announcement noted that Google had responded on the compliance deadline with a letter contesting the agency's "reasoning" but had not yet implemented the requested changes. The U.K. Information Commissioner's Office ("ICO") gave Google until 9/20/13 to comply with its data protection laws; although the deadline has passed, the ICO has not yet announced any further steps. On 12/19/13, Spain's DPA fined Google €900,000 ($1.2 million) for three privacy violations stemming from the unified	10/16/12: Letter issued. 6/20/13: Coordinated enforcement actions initiated against Google. 12/19/13: Fine levied against Google by AEPD. 1/3/14: Fine levied against Google by CNIL.

			policy. The AEPD accused Google of collecting personal information without providing notice of what specific data it collects or the purposes for which Google uses the personal information, and of collecting the information without first obtaining valid consent. On 1/3/14, CNIL levied a record €150,000 fine ($203,571) against Google after the company failed to heed its order to modify its service-wide privacy policy to comply with French law. The penalty is the highest ever handed down by the CNIL's enforcement committee. Google subsequently announced its appeal of the CNIL fine to France's highest administrative court. That appeal remains pending.	
International Privacy Protection Data Security	Singapore Personal Data Protection Commission	Compliance Deadline Announced Advisory Guidelines Issued	The Singapore Personal Data Protection Commission has announced that the country's new Personal Data Protection Act will go into effect on 7/2/14. By that date, all companies operating in Singapore are expected to have completed a variety of compliance measures, including data inventory mapping, process audits, training, and publication of data handling processes. On 9/24/13, the Commission published two sets of advisory guidelines on the interpretation and application of the new law: the first addresses several "key concepts" of the new law such as opt-out consent, notice, purpose limitation, and breach notification, while the second examines the impact of the law on certain specific issues, including collection of IP addresses and the use of cookies. The guidelines, though seen as business-friendly, are purely advisory and have no legal effect. Binding regulations are expected in 2014.	11/20/12: Personal Data Protection Act becomes law. 5/20/13: Data protection authority announces that the Act's main provisions will go into effect in 7/2014. 9/24/13: Advisory guidelines issued.
International Privacy Protection Data Security	European Union Agency for Network and Information Security ("ENISA")	Reports and Guidance Documents Released	ENISA, established in 2004 by EU regulation, released several cybersecurity reports and guidance documents. On 11/25/13, ENISA announced the latest updates to its national cybersecurity strategies map, which details cybersecurity policy amendments in Europe. On 11/27/13, ENISA released a report outlining the possible use of mobile roaming technology in response to cyberattacks on mobile communications networks. On 11/28/13, ENISA released a guide detailing how member states' computer emergency response teams (CERTs) can cooperate with law enforcement to further the EU Directive on attacks against information systems. On 12/11/13, ENISA released CERT	11/25/13: National security map updated. 11/27/13: Report on mobile roaming technology released. 11/28/13: CERTs guide released. 12/9/13: EISAS

			maturity model guidance for governments in the process of assessing the effectiveness of their cybersecurity efforts. On 12/9/13, ENISA released a European Information Sharing and Alerting System (EISAS) feasibility study, which describes a "deployment plan" for the EISAS cybersecurity readiness information-sharing concept and organizational structure. A threat assessment report released 12/11/13 reviewed approximately 250 cyberattacks in 2013 and revealed that mobile and big data have emerged as new cybersecurity battlefields.	feasibility study released. 12/11/13: CERT maturity model guidance released. 12/11/13: Threat assessment report released.
International Privacy Protection Anonymity	German Schleswig-Holstein Data Protection Authority ("ULD")	DPA Order Quashed Appeal Rejected Ruling Issued	A German court rebuffed efforts of Germany's data protection authority, ULD, to apply German data protection law to Facebook. According to the court, although a Facebook office exists in Germany, it only engages in marketing and sales; the European subsidiary where personal data is processed is located in Ireland, so only Irish data protection law applies. On 4/24/13, the ULD's subsequent appeal was rejected by a higher administrative court. In contrast, the Higher Regional Court of Berlin on 1/14/14 affirmed that German data protection law, rather than Irish law, should govern a separate dispute over Facebook's friend-finder feature because Facebook used an in-country subcontractor, and also placed cookies on German users' computers to run applications, which the court ruled was the legal equivalent of Facebook having equipment located in Germany. This ruling could open the door to allow non-European companies to be exposed to Germany's stringent privacy law. It remains unclear how Germany will apply its law to online services such as Facebook going forward.	2/15/13: Opinion issued. 4/24/13: Appeal rejected. 1/14/14: German data protection law held applicable to Facebook.
International Privacy Protection Gaming	U.K. Office of Fair Trading	Principles Released	On 1/30/14, the U.K. Office of Fair Trading ("OFT") released final principles for online and application-based games, including a provision requiring that companies disclose to users whether their personal data will be shared with other parties for marketing purposes. The OFT announced that the online gaming industry must comply with the rules by 4/1/14 or risk enforcement action.	1/30/14: Principles released. 4/1/14: Deadline for compliance.
International Privacy Protection Spam	Canadian Governor in Council	Regulations Issued Regulatory Impact Analysis Statement Issued	On 12/4/13, the Canadian government announced the finalization of the Industry Canada regulations under Canada's anti-spam and anti-malware law ("CASL"). The Canadian government also announced that the bulk of CASL, including the provisions imposing express opt-in consent and form and content	10/22/13: Memorandum of Understanding reached. 12/14/13: Regulations

			requirements for commercial electronic messages, will take effect on 7/1/14. Anti-malware provisions will take effect 1/15/15. A private right of action to bring claims for statutory damages has been deferred until 7/1/17. The Regulations contain definitions of key terms set forth in CASL and enumerate conduct that is exempt from key aspects of the legislation. Industry Canada published together with the finalized IC Regulations a detailed Regulatory Impact Analysis Statement in which it provides guidance on the intended scope of the IC Regulations and the intended interpretation of CASL. On 10/22/13, Canada's Competition Bureau, the OPC, and the Canadian Radio-television and Telecommunications Commission agreed to a memorandum of understanding to cooperate in the enforcement of Canada's new anti-spam law. Under the MOU, the federal privacy office will share personal information only to the extent necessary to meet the requirements for agencies to share information obtained in the course of enforcement activities. The MOU states that none of the agencies is required to communicate information that would violate other legislation under its administration or enforcement responsibility.	issued. 7/1/14: Bulk of CASL takes effect. 1/15/15: Anti-malware provisions take effect. 7/1/17: Private right of action takes effect.
International Privacy Protection	U.K. Information Commissioner's Office	Guidance Issued	On 8/15/13, the ICO published a 58-page "Code of Practice" providing guidelines and advice for responding to requests from data subjects for personal information held by a company. The code explains whether, when, and how a company must respond to such a request and provides a checklist that companies can use to evaluate compliance with the ICO's regulations. Although the guidelines do not appear to alter any substantive obligations of the data controller, they may be a useful resource for clarifying the controller's responsibilities. The ICO also announced it will conduct a "sweep" of websites later in 2013 to evaluate how companies respond to access requests and will publish a report with its findings in 2014.	8/15/13: Guidance issued.
International Privacy Protection	Russian State Duma	Data Protection Law Becomes Effective	A new data protection law went into effect on 10/1/13 requiring consent prior to collection, storage, publication, or use of personal information regarding individuals.	7/5/13: Data protection law enacted. 10/1/13: Data protection law goes into effect.

INTERNATIONAL DEVELOPMENTS AFFECTING U.S. BUSINESSES (continued)

International Privacy Protection	Ukraine Ministry of Justice	Regulations Issued Data Processing Rules Adopted	The Ukrainian Justice Ministry had issued new regulations concerning revised notice and registration requirements for new databases containing personal information. The law's applicability to pre-existing databases is unclear. Companies are no longer required to register databases, but instead must notify the DPA only if intended data processing activities present a special risk to data subjects. Additionally, the new regulation deleted the existing definition of "consent" but failed to provide a new one, making it unclear how to determine whether consent is valid in Ukraine. The regulations also identify a new data protection authority; replacing the State Service on Personal Data Protection is the Ministry of Justice's Office of the Ombudsman. The Commissioner of the Ukraine Parliament for Human Rights is now considered the Ukrainian data protection commissioner. The Ukrainian data protection authority announced that adopted new data processing rules, including (i) a data processing regulation that requires data controllers to notify data subjects about the processing of their personal data within 30 working days; (ii) a monitoring and audit compliance procedures regulation that authorizes the Ombudsman to conduct both announced and surprised audits; and (iii) a notification regulation that requires that data controllers notify the Ombudsman of plans to process High Risk Data and to file formal notification forms within 30 working days after beginning to process such data.	7/22/13: Regulations issued. 1/13/14: New data processing rules adopted.
International Privacy Protection	Malaysian Personal Data Protection Department	Data Protection Law Takes Effect	Malaysia's omnibus Personal Data Protection Act went into effect on 8/16/13, setting out the country's first comprehensive data protection framework. The law's basic principles derive from the EU Data Protection Directive. Violators of the law are subject to criminal penalties including fines up to $155,000 and imprisonment. On 11/15/13, implementing regulations governing data protection principles, registration of data users, fees associated with registration or data access requests, and classification of data users were released with the announcement that the PDPA went into effect. The new data registration rules may have implications for multinational companies if they use "equipment" in Malaysia for the purposes of processing personal data.	8/16/13: Law went into effect. 11/15/13: Implementing regulations went into effect.

International Privacy Protection	Office of the Australian Information Commissioner ("OAIC")	Draft Guidelines Issued	OAIC published draft guidelines for public comment governing a range of data protection and security requirements in Australia in 2013. The new requirements amend regulations referred to as the Australian Privacy Principles ("APPs"), and went into effect on 3/12/14. The APPs cover the collection, use, disclosure, and storage of personal information by Australian businesses and government agencies. The amendments include new requirements that personal information can only be disclosed to an overseas recipient if the disclosing organization has taken reasonable steps to ensure the recipient will not breach the principles. However, this requirement does not apply if the disclosing organization reasonably believes that overseas recipients are subject to similar privacy controls in their own jurisdictions. On 2/21/14, OIAC released guidelines on how it plans to interpret the APPs. The guidance covers topics such as collecting information, direct marketing, information integrity, access to information, and overseas data transfers of personal information. The guidelines draw a distinction between disclosing to an overseas recipient, which would be subject to APP obligations, and mere use of the information by an overseas recipient, which would not be subject to APP obligations. For example, providing data to an overseas cloud service provider would likely be a use, not a disclosure, if a contract requires the cloud service and its sub-contractors only to store the information and leaves control of the information in the hands of the Australian entity. In addition, the guidelines state that the principles will not apply to disclosure to an overseas branch of an Australian company.	Aug.-Sept. 2013: Guidelines issued. 2/21/14: Guidelines released. 3/12/14: APPs went into effect.
International Privacy Protection	South African Parliament	Data Protection Law Passed	On 8/22/13, the South African parliament passed the country's first comprehensive data protection law. The law sets forth notice and consent requirements, breach notification rules, and imposes restrictions on cross-border data transfers. The law also provides a private right of action along with criminal penalties ranging from $1 million fines to imprisonment up to 12 months. Additionally, the law establishes the country's first data protection agency, the Information Protection Regulatory Commission. Companies will have a three-year transition period to comply with the new requirements. The president of South Africa signed the law on 11/19/13.	8/22/13: Data protection law passed. 11/19/13: President signed law.

International Privacy Protection	Chinese Ministry of Industry and Information Technology ("MIIT")	Regulations Issued	On 7/16/13, the MIIT issued new regulations governing telecommunication service providers ("TSPs") and Internet information service providers ("IISPs") that collect and use personal information. The regulations expand the definition of personal information to include any information collected during the provision of telecommunication or Internet information services that would identify the user if used alone or with any other information, along with identity information such as surname, birthday, identity card number, address, and other recorded information about an individual's use of Internet services such as the user's service numbers, account numbers, time, and location. The regulations require TSPs and IISPs to: (1) post collection and use policies at base of business or online; (2) not collect a user's personal information without the user's consent; (3) notify users of the purpose, method, scope of use, retention period, and avenues by which a user can consult or amend personal information, (4) refrain from using personal information for any purpose outside of the stated scope of purpose; and (5) maintain strict confidentiality over personal information. TSPs and IISPs must also adopt specific measures to protect against the disclosure, damage, or loss of users' personal information.	7/16/13: Regulations issued. 9/1/13: Regulations entered into effect.
International Privacy Protection	Office of the Privacy Commissioner of Canada ("OPC")	Enforcement Reports Issued	The OPC released an enforcement report finding violations of PIPEDA by a dating website that made its customers' personal information available to more than 50 affiliated sites without consent. OPC also found in a separate enforcement report that a bank violated PIPEDA by informing a customer that he needed to provide his driver's license number to pick up a replacement credit card. The bank incorrectly stated that this information was required in order to comply with Canada's Proceeds of Crime (Money Laundering) and Terrorist Financing Act. Both enforcement reports were issued 10/22/13.	10/22/13: Enforcement reports issued.
International Privacy Protection	Institute of Access to Information and Data Protection ("IFAI")	Guidelines Issued	Mexico's data protection authority, IFAI, published nonbinding guidelines for data security that implement the data security provisions of the country's framework data protection statute, the Federal Law on the Protection of Personal Data in the Possession of Private Parties. In the guidelines, IFAI recommended that companies adopt personal data security management systems based on a four-part "Plan-Do-Verify-Act" process. The process	10/30/13: Guidelines issued.

			involves identifying key security objectives and conducting a risk analysis, implementing the necessary policies, procedures, and plans to help achieve these objectives, auditing and evaluating whether policies, procedures, and plans are achieving these objectives, and taking corrective action and other remediation measures to improve security, including training relevant personnel.	
International Privacy Protection	Supreme Court of Canada	Statute Invalidated	On 11/15/13, the Supreme Court of Canada invalidated the province of Alberta's Personal Information Protection Act ("PIPA") on the basis that it improperly infringes upon the constitutional rights of unions. The court stated that the provisions prohibiting the collection, use, and disclosure of personal information without consent do not permit unions to fully exercise their rights, particularly the use of picketing. The ruling gave the province 12 months to redraft the statute.	11/15/13: PIPA invalidated. 11/15/14: Deadline to redraft PIPA.
International Privacy Protection	French Data Protection Authority (CNIL)	Recommendation Adopted	The CNIL governing board issued an official recommendation on 12/17/13 which expands on previous cookie-related guidance that CNIL issued in 2011 and revised in 2012. The recommendation states that companies must obtain prior consent for: cookies linked to banner advertising on sites; social networks' cookies linked to "sharing" buttons that collect user information without asking for prior consent; and certain site traffic measurement cookies. The guidance summarizes several other requirements for consent, including that the user must be able to withdraw consent for cookies at any time, and that consent is valid for only 13 months, after which the user must give consent again. The recommendation also provides certain exceptions for cookies that do not require consent, such as those used for shopping cart functions and load-balancing.	12/17/13: Recommendation released.
International Privacy Protection	Art. 29 Working Party	Work Program Released	The Article 29 Working Party intends to step up enforcement coordination efforts during 2014 and 2015, according to the work program posted in December on its website. The Working Party also included details on the work that its subgroups will focus on, such as issuing guidance on cloud computing and device fingerprinting and considering the proposed regulation's impact on tools to transfer personal data outside the EU.	

INTERNATIONAL DEVELOPMENTS AFFECTING U.S. BUSINESSES (continued)

International Privacy Protection	U.K. Information Commissioner's Office ("ICO")	Code of Practice Released	On 2/25/14, the ICO published its updated privacy impact assessments ("PIAs") code of practice targeted at businesses and other organizations in the U.K. that handle personal information. A PIA is a tool that assists organizations to identify the most effective way to comply with their obligations under the U.K.'s Data Protection Act and to meet individuals' expectations of privacy. The code of practice recommends the privacy issues that organizations should take into account when planning projects that use personal information.	2/25/14: Code of practice published.
International Privacy Protection	FTC U.K. Information Commissioner's Office ("ICO")	Memorandum of Understanding Released	The FTC and U.K. ICO agreed in a Memorandum of Understanding to cooperate in cross-border enforcement efforts to protect personal information. The MOU notes that the FTC is allowed by law to share information involving cross-border fraud with foreign consumer protection agencies, subject to statutory safeguards.	3/6/14: Memorandum of Understanding released.
International Privacy Protection	Japanese Ministry of Economy, Trade, and Industry	Code of Practice Released	The Japanese Ministry of Economy, Trade and Industry has released a code of practice on how businesses should notify consumers about the collection and use of personal data. The code of practice recommends that businesses: outline the service the business will provide; detail what data are collected and how; detail how personal data will be used; disclose whether personal data have been shared; explain whether consumers can stop collection or seek correction to personal data already collected; disclose contact information; and explain to consumers how long the personal data will be retained and how it will be destroyed.	4/1/14: Code of practice released.