Bloomberg Law Reports® Privacy & Information

Traveling the New Road to Data Privacy Regulation in the United States: An Examination of Recent U.S. Data Privacy Considerations and Proposed Legislation, Including Safe Harbors Contemplated by Congress

James A. Sherer, Andrew J. Cosgrove and Victoria A. Redgrave, Redgrave LLP

A spate of recent – and renewed – interest in data privacy by the U.S. Government should give those organizations that collect sensitive and personally identifiable information from individual consumers reason to pause. And while two proposed Senate and House Bills are still in committee, their combined import is clear: the U.S. Government is in the process of stepping-up its regulation of U.S. organizations' use of personal data. So-called opt-in agreements and End User License Agreements ("EULAs") will no longer suffice; U.S. consumer data privacy has attracted new government interest, and organizations who fail to take pending regulations seriously could face severe consequences and civil penalties.

U.S. Data Privacy Laws – A Slow Evolution

Almost anyone using the Internet during the early 1990's would agree that, at the time, the U.S. government chose to view privacy issues as a casualty of the "unrestrained growth of the Internet," which was "an exciting new medium for free expression and commerce."[1] Over the next decade, this approach morphed somewhat, but instead of directing the entirety of Internet traffic, the government allowed organizations to create and implement self-imposed "enforceable codes of conduct to govern commercial privacy."[2] Yes, there were some singular, more hard-line exceptions, such as the 1998 Children's Online Privacy Protection Act ("COPPA")[3], but for the most part the onus of managing data privacy was on the organizations themselves.

As the United States moved into the 21st century, there were new government-led attempts to address data privacy regulation with a more general focus; however, few of these attempts ultimately proved successful. Among them:

- The 2005 Data Accountability and Trust Act ("DATA"), which was introduced by the House in the 109th Congress and expired before it passed.
- In 2007, the 110th Congress reconsidered the original "DATA" through H.R. 958, which also sought to protect consumers by requiring reasonable security policies and procedures to protect computerized data containing personal information. The bill was cleared from the Congressional books after it failed to pass by session's end.

- In 2007, the Senate considered S.495, the Personal Data Privacy and Security Act of 2007, "a bill to prevent and mitigate identity theft, to ensure privacy, to provide notice of security breaches, and to enhance criminal penalties, law enforcement assistance, and other protections against security breaches, fraudulent access, and misuse of personally identifiable information."[4] This bill suffered the same fate as the "DATA" bills. It was placed on the Senate Legislative Calendar under General Orders on May 23, 2007, and went no further.

In the meantime, the general *lassiez-faire* approach to data privacy eventually led us to the (more) current data privacy practice that U.S. consumers experience today: the ability to "opt-in" or "opt-out" of privacy protections upon the terms and conditions set forth in long, potentially confusing agreements. Although these practices demonstrate an evolution in sophistication from 1990's standards, they stand in stark contrast to those of the European Union, which by 1995 had passed an omnibus Data Protection Directive,[5] which was subsequently implemented by the EU's member countries.[6]

Are the 2010's the Decade of U.S. Consumer Privacy Reform?

As the U.S. approaches the middle of 2011, incidents such as the Sony security breach that resulted in the release of the personal information (including some credit card data) of close to 100 million PlayStation users have given lawmakers a renewed interest in consumer data privacy. In addition to the Sony breach, the recent concerns around Apple's iOS and Google's Android location-based services[7] have also drawn government and public interest. When combined with more general Federal, State and International issues, and the rapid advancement and use of technology, this collection of events has catalyzed a series of governmental actions that give a clear indication of pending reform:

- In April, 2010, Gary Locke, the U.S. Secretary of Commerce, formed an Internet Policy Task Force ("IPTF").
- On December 1, 2010, the Federal Trade Commission ("FTC") issued a privacy report endorsing a "Do Not Track" mechanism to "Facilitate Consumer Choice about Online Tracking."
- On December 16, 2010, the Department of Commerce unveiled a policy framework (known as the "Green Paper") "aimed at promoting consumer privacy online while ensuring the Internet remains a platform that spurs innovation, job creation, and economic growth."[8]
- On April 11, 2011, the Senate Committee on Commerce, Science, and Transportation introduced a bipartisan bill sponsored by Senators John Kerry (D-Mass.) and John McCain (R-Ariz.), S.799: Commercial Privacy Bill of Rights Act of 2011 – aimed at establishing a regulatory framework for the comprehensive protection of personal data for individuals under the aegis of the Federal Trade Commission.
- On May 5, 2011, the House Committee on Energy and Commerce's Subcommittee on Commerce, Manufacturing, and Trade held a hearing on the "Threat of Data Theft to American Consumers."
- On May 10, 2011, representatives from Google and Apple were called to testify at a hearing called "Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones and Your Privacy" before the Senate Committee on the Judiciary, Subcommittee on Privacy, Technology and the Law, chaired by Senator Al Franken (D-Minn.).[9]

While new data privacy legislation has yet to be enacted, this fast-paced succession of events clearly illustrates that the U.S. government is paying atten-

tion. The writing is on the wall, and more importantly, as one article put it, the "[p]olitical will is there."[10] Pressure is being applied to the issue of consumer data privacy from the executive and legislative branches, which means organizations of all types should begin marshaling resources and considering safe harbors if they want to be prepared for the inevitable change.

Recent Events May Offer a Roadmap for Organizational Compliance

As we wait to see how the specifics of U.S. consumer privacy regulations play out, organizations can (and should) begin assembling a roadmap based on the perspectives provided through events like those referenced above. For the purpose of this paper, we will look at a subset of these in greater detail.

When the Federal Trade Commission released its preliminary privacy report on December 1, 2010, the FTC provided consumers, businesses and policymakers with a framework for managing data privacy that included three key recommendations:

1. *Privacy by Design*: directing organizations to design products, services and process with privacy protections in mind;
2. *Simplified Choice*: directing organizations to make consumer options for opting into or out of personal data collection easier; and
3. *Greater Transparency*: requiring organizations to clearly disclose their data collection methods.[11]

While this FTC report did not provide any specific guidance regarding the operation of new Safe Harbors for data privacy or FTC enforcement of any new data privacy regulations, it did discuss the U.S.-EU Safe Harbor Framework, and made mention of the COPPA Safe Harbor Program.

The Department of Commerce's "Green Paper," released several weeks later, offered guidance for additional dimensions of managing sensitive information. In an attempt by the Department of Commerce to protect consumer trust in the Internet economy while still promoting innovation, their paper, officially entitled "Dynamic Privacy Framework for Commercial Data," offered the following recommendations:

1. The Adoption of Fair Information Practice Principles ("FIPPs") to promote informed consent and protect the "privacy of personal information in commercial contexts not covered by an existing sectoral law;"
2. The Use of FIPPs to expand interoperability between U.S. and other international data privacy regimes;
3. The continued maintenance of U.S. commercial data privacy policy flexibility to allow voluntary industry codes of conduct (including the development of a Safe Harbor for organizations);
4. The creation of a Privacy Policy Office within the Department of Commerce; and
5. The setting of a national standard for notifications following security breaches which involve personal information in the commercial context. [12]

Proposed Federal Privacy Legislation

While it may not have been addressed by the FTC Report, the third "Green Paper" recommendation clearly indicates that there is discussion of "legislation that would create a Safe Harbor for companies that adhere to appropriate voluntary, enforceable codes of conduct that have been developed though open, multi-stakeholder processes."[13] This Safe Harbor would operate "against FTC enforcement for practices defined by baseline data privacy or volun-

tary enforceable codes"[14] and could be considered "ample incentive to participate in developing voluntary codes"[15] which would then be subject to FTC approval.

The Commercial Privacy Bill of Rights Act, proposed in April of 2011 by Senator John Kerry (D-Mass.) and Senator John McCain (R-Ariz.), takes the ideas presented in the FTC Report and the Commerce "Green Paper" a step further. Senator McCain has declared that this bill would protect the "fundamental right of American citizens, that is the right to privacy."[16] The bill claims that individuals "interacting with others engaged in interstate commerce have a significant interest in their personal information, as well as a right to control how that information is collected, used, stored or transferred."[17] This proposed legislation outlines a suggested structure for an organization's use of private information based on three key areas:

1. Security and Accountability organizational requirements, including a process to respond to non-frivolous individual inquiries, as well as a description of the organizations' means of compliance with the Act's requirements upon request from the FTC or a safe harbor program;[18]
2. Transparency organizational requirements, such that customer participation in data collection is done by "clear and conspicuous" mechanisms, specifically requiring "opt-in consent" for a variety of information uses; [19] and
3. Data Minimization organizational requirements, which would limit the collection of an individual's information to that which is "reasonably necessary" as defined by the Act.[20]

Additionally, the proposed Commercial Privacy Bill of Rights Act of 2011 also offers insight into the types of entities and information that could be covered under such legislation:

- The bill would regulate any person or organization who "collects, uses, transfers, or stores covered information concerning more than 5,000 individuals during any consecutive 12-month period" and who is subject to the jurisdiction of the FTC, a common carrier subject to the Communications Act of 1934, or is a non-profit – including those non-profits exempt from taxation under section 501(a) of the Internal Revenue code of 1986.[21]
- Noticeably absent is regulation specific to any government use of private or covered information.
- The bill defines covered information to include "Personally identifiable information" (PII), "Sensitive personally identifiable information," "unique identifier information" (UII) and "any information collected in connection with PII or UII that may be used to identify an individual."[22]

Less than a month after Senator Kerry and Senator McCain proposed their bipartisan Privacy Bill of Rights, the House Committee on Energy and Commerce Subcommittee on Commerce, Manufacturing, and Trade held a hearing on "The Threat of Data Theft to American Consumers." During this hearing, the Committee sought to examine "risks related to data breaches, the state of ongoing investigations, current industry data security practices, and available technology."[23] And in a prefatory memo to the hearing, Committee Members reiterated concerns about "the confusing and often overlapping or contrary patchwork of State notification laws,"[24] and specifically stated that, following the hearings, Chairman Mary Bono Mack would introduce a "data security bill based on the unsuccessful 'DATA' legislation from the 109th Congress" which would aim to do the following:

1. Require entities that hold personal information to establish and maintain ap-

propriate security policies to prevent unauthorized acquisition of that data;
2. Require companies to notify consumers in the event of a breach of personally identifiable information that results in a reasonable risk of identity theft or fraud;
3. Impose special requirements on information brokers, those that compile and sell consumer data to third parties, including assuring accuracy of their information, allowing consumer access to their records and the ability to correct inaccurate information;
4. Supersede State data breach and notification laws but permit enforcement by State Attorneys General with an aggregate cap on damages;
5. Preempt similar State laws to create a uniform national standard for data security and breach notification;
6. Mandate reasonable security practices for paper records containing personally identifiable information;
7. Permit an information broker to include intentionally false information in a database if used for fraud detection purposes and the information is identified as inaccurate;
8. Allow for a delay in breach notification for law enforcement or national security purposes; and
9. Add passport numbers and military ID numbers to the definition of personal information. [25]

Lastly, there were clear indications of U.S. Government interest demonstrated in the testimony that Apple Vice President Bud Tribble and Google Director of Government Relations and Public Policy Alan Davidson provided before the Senate Judiciary Subcommittee on Privacy, Technology and the Law on May 10, 2011. The issues that drove this inquiry focused on the question of who is watching out for the individual consumers – those customers who click through the agreements in the current "opt in" framework that "tends to leave 'privacy to the lawyers and their process-based "click if you 'consent' to the privacy policy"' approach."[26] Under this method, which is currently employed by nearly every organization operating only in the U.S., the common sentiment is that the only people who read the releases are the lawyers who draft them. Even the media has taken notice, and parodied that very practice in a recent South Park episode where character Kyle neglects to read the full end user license agreement (the so-called "EULA") from an iTunes update, and is subjected to a number of unsavory machinations by Steve Jobs.[27]

In the wake of these events, Ken Johnson, a senior adviser for Representative Mack, held out hope that the recent data breaches might force legislators to "put aside political squabbles, and do what's best for consumers."[28] Indeed, political capital is being spent to pursue these issues, and when high-profile data breaches and issues are added to already existing pressure from the EU and Europeans who feel that U.S. requests are attempts to create "see-through Europeans," 2011 marks a confluence of circumstance that could lead to real, lasting change for organizations that collect, handle or manage U.S. consumer data.

Charting a Course for the Future

As discussed above, when it comes to consumer data privacy, the current U.S. business environment is currently comprised largely of self-regulating organizations that themselves deal with a conglomeration of Federal, State and local rules. This has led organizations to rely on the presentation of "opt-in" or "opt-out" agreements to consumers, in coordination with overly-complicated EULAs, and to the inconsistent collection of private information. Although consumer data privacy may be loosely regulated today, it is certainly slated to gain a considerable amount of further regulation by year's end.

The future is not difficult to imagine. Indeed, for a contrarian model of the type contemplated by the proposed legislation, U.S. organizations have only to look across the Atlantic to see how the EU Privacy Directive has brought together compliance between different nations – countries with different norms, languages and models of conducting business. The Commerce Department's "Green Paper" certainly looked to the EU Privacy Directive for guidance, and while many U.S. organizations have expressed (not surprisingly) that new efforts at regulating privacy could stifle innovation without having net positive effects, government actions over the past two years (again) demonstrate that the United States is preparing to pave new roads in data privacy protection.

Indeed there have been previous government "false starts" in this arena. But consumers are "wising up" to the personal risks they face regarding the release of personally identifiable information. The U.S. Government's sophistication is growing as well, and recent events and efforts have paved the way for relatively quick action that would demonstrate a powerful response to the concerns and vulnerabilities of American citizens. When such actions occur, the first targets will likely be those organizations that have not changed the language of their "opt-in," "opt-out," or EULA "click boxes." The second targets will likely be organizations lacking strong internal reporting lines for the collection and use of individual consumer data.

It is absolutely correct that any single organization *could* wait until legislation is enacted, choosing to believe that implementation of any Act will grant sufficient time for an organization to execute an appropriate response. However, for most organizations, this is simply a myopic approach, given the substantial time required to determine: (1) what information an organization collects, and how; (2) where the information is stored, and by what means; (3) how existing (or proposed) records and information management policies intersect with legal obligations (themselves exceptions to the proposed Senate Bill) and; (4) what, if any, efforts an organization will take to align itself with one of the proposed Safe Harbors. So, while some may await final action, perhaps for a little while longer, a savvy organization will find the time to ask the harder questions and begin charting their course today.

James A. Sherer is a Partner at Redgrave LLP's Washington, D.C. office; Andrew J. Cosgrove is an attorney in Redgrave LLP's Minneapolis office; Victoria A. Redgrave is a Managing Partner in Redgrave LLP's Washington, D.C. office.

---

[1] The Department of Commerce - Internet Policy Task Force, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*, Executive Summary (2010) (http://www.ntia.doc.gov/reports/2010/iptf_privacy_greenpaper_12162010.pdf).

[2] *Id*.).

[3] CHILDREN'S ONLINE PRIVACY PROTECTION ACT OF 1998, H.R.3783, 105th Cong. (1998).

[4] THE PERSONAL DATA PRIVACY AND SECURITY ACT OF 2007, S. 495, 110TH CONG. (*discussion at* http://thomas.loc.gov/cgi-bin/bdquery/z?d110:s.00495:).

[5] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. (http://ec.europa.eu/justice/policies/privacy/law/index_en.htm).

[6] *See* European Commission, Status of Implementation of Directive 95/46 on the Protection of Individuals with Regard to the Processing of Personal Data (http://ec.europa.eu/justice/policies/privacy/law/implementation_en.htm (last updated Aug. 6, 2010) (listing national laws).

[7] C. Albanesius, *Senator Has 'Serious Doubts' About Privacy of Google, Apple Location Apps*, PCMAG.COM, May 10, 2011 (http://www.pcmag.com/article2/0,2817,2385150,00.asp)

[8] U.S. Department of Commerce: Commerce Department Unveils Policy Framework for Protecting Consumer Privacy Online While Supporting Innovation (http://www.commerce.gov/news/press-releases/2010/12/16/commerce-department-unveils-policy-framework-protecting-consumer-priv).

[9] N. Bilton, *Who Could Become the Data Sheriff?* Bits - The New York Times, May 12, 2011 (http://bits.blogs.nytimes.com/2011/05/12/who-could-become-the-data-sheriff/?src=tptw).

[10] D. Etherington, *Senate Hearing: Apple, Google and the Future of Mobile Privacy*, Gigaom.com, May 10, 2011 (http://gigaom.com/2011/05/10/senate-hearing-apple-google-and-the-future-of-mobile-privacy/).

[11] The U.S. Federal Trade Commission, *A Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* (Dec. 1, 2010) (http://www.ftc.gov/os/2010/12/101201privacyreport.pdf).

[12] The Department of Commerce - Internet Policy Task Force, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*, at p. 22 (2010) (http://www.ntia.doc.gov/reports/2010/iptf_privacy_greenpaper_12162010.pdf).

[13] *Id*. at p. 72.

[14] *Id*. at p. 29.

[15] *Id*. at p. 43.

[16] D. McCullagh, *US privacy Bill of Rights exempts govt*, CNET News.com (April 14, 2011) (http://www.zdnet.com.au/us-privacy-bill-of-rights-exempts-govt-339313214.htm).

[17] *Id*. at §2.

[18] *Id*. at §102.

[19] *Id*. at §201.

[20] *Id*. at §301.

[21] *Id*. at §401.

[22] *Id*. at §3.

[23] Majority Committee Staff, The U.S. House Committee on Energy and Commerce, *Internal Memorandum regarding Hearing on "The Threat of Data Theft to American Consumers*", p. 1 (May 2, 2011) (http://republicans.energycommerce.house.gov/Media/file/Hearings/CTCP/050411/Memo.pdf).

[24] *Id*. at p. 2.

[25] *Id*. at p. 3.

[26] The Department of Commerce - Internet Policy Task Force, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*, p. 25 (Dec. 16 2010) (http://www.ntia.doc.gov/reports/2010/iptf_privacy_greenpaper_12162010.pdf).

[27] T. Parker, *HumancentiPad*, South Park Season 15, Episode 210, first aired on Comedy Central April 27, 2011 (http://www.southparkstudios.com/full-episodes/s15e01-humancentipad).

[28] N. Bilton, *Who Could Become the Data Sheriff?* Bits - The New York Times, May 12, 2011 (http://bits.blogs.nytimes.com/2011/05/12/who-could-become-the-data-sheriff/?src=tptw).