Proskauer

Everybody Likes Free Stuff: Draft Privacy Legislation Seeks To Enhance Consumer Protections Without Disrupting Ad-Supported Internet Business Model

May 11, 2010

A draft Congressional bill released Tuesday, May 3 would enhance consumer privacy protections both online and offline and establish a national framework for the collection, use and security of consumer information, superseding state law requirements regarding the collection, use and disclosure of the information it covers.

Among other things, the legislation would require that covered entities revamp their privacy notices and information security programs, provide consumers a right to opt-out of certain collection, use and disclosure of consumer information, obtain consumers' affirmative consent under certain circumstances, and protect the security of consumer information.

Congressmen Rick Boucher (D, Va.) and Cliff Stearns (R, Fl.) released the bill. Mr. Boucher is the Chairman of the House Subcommittee on Communications, Technology and the Internet, and Mr. Stearns is the subcommittee's Ranking Republican Member. The bill's sponsors have invited comments on the draft legislation with an aim towards introducing formal legislation during a House subcommittee hearing sometime in the next month or two. Entities that would be most impacted by the legislation include those that collect data from consumers, either online or offline, and use it for marketing purposes or share it with third parties. Interested entities should strongly consider commenting on the legislation before it is formally introduced. The bill's sponsors have requested comments on the draft by June 4th, and stakeholder meetings may also be scheduled to discuss the draft and receive comments.

In their executive summary of the bill, the drafters stated their underlying intent for the bill to promote the greater use of the Internet for e-commerce and cloud computing by giving consumers greater control over their privacy and promoting transparency regarding the collection, use and sharing of information. The bill recognizes the importance of online advertising in supporting free online content and services and attempts to extend privacy protections without disruption of this business model.

Privacy Notice Requirements With "Opt-Out" Framework

The legislation would codify what is already the industry standard "notice and opt-out" system for the collection and use of most kinds of "covered information." In other words, covered entities would have to give consumers a right to opt-out of the collection and use of their information, but would only have to obtain a consumer's affirmative consent in certain circumstances. Covered information includes, among other things, a consumer's:

- name,
- address,
- phone and fax number,
- e-mail address,
- any government-issued identification number (such as a Social Security number or a driver's license number),
- any financial account number,
- biometric data,
- a unique identifier (including a customer number or IP address used to link data to a specific individual or his or her computer, device or application), and
- preference profile (which is defined as a list of information or preferences associated with a specific individual, or computer or device owned or used by a particular user).

The collection and sharing of non-personally identifiable aggregate information and information that has been rendered anonymous is not covered by the proposed legislation. However, to render data anonymous, it must be non-identifiable with respect to both the individual and a computer or device owned or used by a particular user. The inclusion of IP addresses in the definition of covered information, if enacted, would make clear that at least under some circumstances an IP address is considered personally identifiable information, thus ending this debate among industry participants and courts in the U.S. As written, an IP address would be covered by the legislation if it is "used to collect, store, or identify information about a specific individual or a computer, device, or software application owned or used by a particular user or that is otherwise associated with a particular user." However, it remains unclear whether this definition would include a dynamically assigned IP address, i.e., one that is assigned to a different computer or device at different times.

The legislation also does not apply to small businesses, specifically entities that collect covered information from fewer than 5,000 people per year, none of which is sensitive information (as defined).

Whereas currently, only California and a few industry or data-specific laws require a company to have a privacy policy, this bill would establish a federal statutory requirement to have an online privacy policy, as well as an offline privacy policy under certain circumstances. In order to collect, use or disclose "covered information," either online or offline, an entity would first have to make available a written privacy notice before collection. In the online context, the notice would have to be posted clearly and conspicuously and be accessible by a direct link from the Website homepage.

The privacy notice would have to include, among other requirements:

- the identity and contact information of the entity collecting the information;
- a description of the information being collected;
- how that information is collected;
- the purpose of the collection and use of the information;
- how the information is stored, for how long, and how it is disposed;
- how the information may be combined with other information from other sources;

- the purposes for which information may be disclosed, and to which types of third parties;
- options consumers have for accessing and/or limiting the information the entity collects or discloses.

If the legislation's privacy notice requirements have been satisfied, and consumers have been given a right to opt-out of the collection and use of their information (other than for transactional or operational purposes, where an opt-out right is not required), the consumer is deemed to have consented to such collection and use of information unless the consumer specifically declines consent.

The FTC's enforcement position has long been that material adverse retroactive changes to privacy policies require consumer opt-in, if the new policy is to be applied to information collected under the old policy. This bill would make this statutory law by requiring that if material changes are made to a privacy policy, the express affirmative consent of the consumer is necessary before applying the new policy to previously collected information, including the disclosure of information the consumer would not reasonably expect to have been shared with third parties under the terms of the prior privacy policy.

Exceptions to the Notice Requirement

There are some important exceptions to the notice requirements. For one, the notice requirements would not apply to name and contact information collected offline for use only by the entity collecting it. This exception is especially helpful to an entity that only collects consumers' name and contact information (and not other information) in stores, on the phone, or at events, and only for its own use. Second, the legislation's notice requirements would not apply to any covered information that is collected offline for transactional or operational purposes. This exception is helpful to entities that do not use information they collect from consumers offline for marketing purposes.

Opt-In Requirements for Certain Data

The legislation would require a consumer's express consent for the disclosure of covered information to an entity's unaffiliated entities. This opt-in requirement would not apply to disclosure to service providers for the purposes of effecting a transaction between the consumer and the entity that collected the information, provided that the service provider has agreed contractually to certain use and confidentiality restrictions.

Another exception to the opt-in requirement is made for "individually managed preference profiles" when certain notice and opt-out mechanisms are employed. This exception supports the online advertising industry by enabling web sites to share consumer data with online advertising networks without consumer opt-in, subject to requirements which are closely in line with measures that the online ad industry has already adopted through self-regulation. In particular, the notice and opt-out mechanism must be established so that: (1) the opt-out choice is protected from accidental deletion (e.g., "opt-out cookies" that can inadvertently be deleted), (2) data is deleted or made anonymous within 18 months, (3) a notice or seal is prominently displayed on the entity's Web site and on or near targeted advertisements, with a link to information about behavioral advertising and how consumers can opt-out, and (4) the advertising network with which the information is shared does not disclose the information outside the network without the consumer's express consent.

Before collecting or disclosing "sensitive information," either online or offline, an entity must make available its privacy policy and obtain the express affirmative consent of the individual. "Sensitive information" includes information relating to an individual's medical records, race, ethnicity, religion, sexual orientation, financial records, or precise geolocation. Express affirmative consent is also required prior to the collection or disclosure of all or substantially all of an individual's online activity. A likely example of this would be deep packet inspection conducted by an ISP.

Information Accuracy and Security Requirements

The bill would require covered entities to establish reasonable procedures to assure the accuracy of covered information. However, the draft legislation does not explain how a company may fulfill this requirement For example, must a company update consumer address information by appending updated information from a data aggregator? Can a company rely on the accuracy of consumer information recently provided by the consumer? For how long? Although the legislation itself does not answer these questions, the Federal Trade Commission ("FTC") may promulgate rules under the Act that provide further guidance.

The proposed legislation also requires covered entities and their service providers to establish, implement and maintain appropriate administrative, technical and physical safeguards to ensure the security, integrity and confidentiality of covered information and to protect it against anticipated threats and hazards, unauthorized access, loss, misuse, alteration or destruction. The wording of the draft legislation mirrors the wording of the Safeguards Rule under the Gramm-Leach Bliley Act, and it is also similar to relatively new data security regulations in Massachusetts as well as other state data security laws. However, the draft legislation is significantly broader than existing laws in the United States since it applies to mere contact information of consumers, such as their names, email addresses, phone and fax numbers, and postal addresses. This broad scope of the legislation, if enacted, would require most companies to expand the scope of their information security programs. However, under the draft legislation, appropriate security measures may be defined according to the "sensitivity" of information. Therefore, the FTC could exercise its rulemaking power under the legislation to require limited data security measures for mere consumer contact information.

Finally, the legislation would require certain breach response measures, such as measures to mitigate the harm arising from a security breach of consumer information. However, notably, the legislation does not require notification to consumers of security breaches. Whether or not the legislation would preempt the 46 existing state breach notification laws, thereby essentially mooting them without replacing them on the federal level, depends on an interpretation of the legislation's preemption provision which, as discussed below, is broadly written.

Enforcement

The bill provides for enforcement by the FTC under the Federal Trade Commission Act, with violations considered an unfair or deceptive act or practice. The legislation would also be enforced by state Attorneys General or consumer protection agencies. No private right of action would be permitted. Interestingly, common carriers subject to the federal Communications Act regulated by the Federal Communications Commission are deemed subject to the jurisdiction of the FTC.

Preemption and Affect On Other Laws

This bill would expressly supersede state law requirements concerning the collection, use or disclosure of covered information. Read literally, this legislation could replace state laws concerning social security number protection, data security, breach notification, and data disposal, as well as state financial and medical privacy laws. It is unclear whether this bill is meant to be read this broadly, but it is hoped that new versions of the legislation will make this more clear.

The bill would have no impact on certain other federal privacy and data security laws like the Gramm-Leach-Bliley Act, Health Insurance Portability and Accountability Act, Communications Act of 1934, Children's Online Privacy Protection Act, and Controlling the Assault of Non-Solicited Pornography and Marketing Act. Where these laws are inconsistent with the proposed legislation, it remains to be resolved which standard would apply.

* * *

Special thanks to Robert Forbes, an Associate in Proskauer's Los Angeles office and a member of the Privacy & Data Security Practice Group, for his assistance in the preparation of this article.

Related Professionals

- **Jeffrey D. Neuburger**
  Partner
- **Anthony J. Oncidi**
  Partner

- **Lary Alan Rappaport**
- **Nolan M. Goldberg**
  Partner
- **Scott P. Cooper**