High-Level Points Regarding the U.S. Privacy and Data Security Landscape

By:Faith D. Kasparian
January 28, 2016

I. Introduction

Unlike other countries, in the United States (despite repeated legislative efforts), there is no omnibus federal privacy or data security law. However, there are state privacy and data security laws as well as a number of federal sector-specific privacy laws. Examples of federal sector-specific privacy laws include the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), 42 U.S.C. § 1320d *et seq.*, (healthcare sector); the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 *et seq.* (financial sector); and the Children's Online Privacy Protection Act, 15 U.S.C. § 6501, *et seq.* ("COPPA") (children's privacy). State and federal laws that generally prohibit unfair and deceptive trade practices (such as the Federal Trade Commission Act and state analogs) also may apply to privacy harms, as they have been used to combat privacy-related unfair and deceptive business practices. But, there is no omnibus, one-size-fits-all, federal legislative umbrella that can be looked to for universal guidance. Consequently, in addition to complying with any applicable state and federal sector-specific privacy laws, it is important for businesses to make reasonable attempts to implement a "best practices" privacy framework upon which management can rely in the event that a third party challenges a company over its approach to data centric privacy-related matters.

II. General Best Practices Privacy Framework

The Federal Trade Commission (FTC) issued a privacy report in 2012 that sets forth a general "best practices" framework with respect to protecting consumer information. The full report is available here. There are three primary components to the framework: (A) Privacy By Design; (B) Simplified Consumer Choice; and (C) Transparency.

A. PRIVACY BY DESIGN

Companies should:

- promote consumer privacy throughout their organizations and at ***every*** **stage of the development of their products and services.**
- incorporate substantive privacy protections into their practices, such as data security, reasonable collection limits, sound retention and disposal practices, and data accuracy.
- maintain comprehensive data management procedures through the life cycle of their products and services.
- collect only the data needed for a specific business purpose.
- retain data only as long as necessary to fulfill that purpose (*i.e.*, major search engines have shortened retention periods for search data).
- implement reasonable procedures to promote data accuracy.

- implement and enforce procedurally sound privacy practices by conducting ***privacy training*** and ***privacy reviews*** of new products and services.
- assign personnel to oversee privacy issues ***from the nascent stages*** of research and development.
- exercise caution before releasing data ***presumed to be anonymous*** for research or other purposes and take steps to minimize linkability of data.

B. SIMPLIFIED CONSUMER CHOICE

1. Companies should also provide consumers with choice before collecting and using consumer data for practices that are not (i) consistent with the context of the transaction or the company's relationship with the consumer, or (ii) required or specifically authorized by law.
2. By way of example, but not limitation, the following practices would not require consumer choice:

- **Product Fulfillment:** Collect contact information to ship requested product.
- **Internal Operations:** Satisfaction surveys to improve service, collecting data about visits/click-through rates to improve site navigation, frequency capping and similar advertising inventory metrics, etc. However, "internal operations" would ***not include the sharing of data with third parties in order to improve existing products or services (which practice would involve consumer choice).***
- **Fraud Prevention:** Offline retailers check drivers' licenses when consumers pay by check or use video cameras. Online businesses may scan web server logs to detect fraud, deleting the logs when they are no longer necessary and engage in practices to prevent security attacks.
- **Legal Compliance and Public Purpose:** Sharing data with law enforcement in response to subpoena; business reporting a consumer's delinquent account to a credit bureau.
- **Most First-Party Marketing:** Online retailer that recommends products based on consumer's prior purchases on the website; offline retailer offering a coupon (including by mail or e-mail) for baby formula to a frequent purchaser of diapers.

3. By contrast, the following "First-Party Marketing" practices ***would require*** consumer choice:

- **Tracking consumers across other parties' websites** (whether through deep packet inspection, social plug-ins, http cookies, web beacons or other types of technology).
- **Allowing marketing by the first-party's affiliates.** Unless the affiliate relationship is clear to consumers, ***affiliates are third parties.***
- **Collecting sensitive data** (i.e., Social Security number, or financial, health, children's, or geolocation information) for first-party marketing.

4. Additionally, examples of other practices that ***would require*** consumer choice include:

- Online behavioral advertising.
- Sharing data with a third party (other than a service provider acting on the company's behalf, including a business affiliate unless the affiliate relationship is clear to consumers though common branding or similar means).
- Allowing a third party, other than a service provider, to collect data about consumers visiting the site.

5. For practices requiring choice, companies should offer the choice ***at a time and in a context*** in which the consumer is making a decision about his or her data.
6. Companies should provide prominent disclosures and obtain ***affirmative express consent*** before:

- Using consumer data in a ***materially different manner*** than claimed when the data was collected; or
- Collecting sensitive data for certain purposes (including marketing).

7. Companies must provide ***prominent disclosures*** and obtain ***affirmative express consent*** before using data in a materially different manner than claimed when the data was collected. Examples of ***materially different*** use include:

- Social networking site changes its policy of keeping profile information private.
- Retailer changes stated policy of not sharing customer data with third parties.

C. TRANSPARENCY

- Companies should increase the transparency of their data practices.
- Privacy notices should be clearer, shorter, and more standardized to enable better comprehension and comparison of privacy practices.
- Companies should provide reasonable access to the consumer data they maintain; the extent of access should be proportionate to the sensitivity of the data and the nature of its use.
- In order for consumers to make informed decisions, companies should expand their efforts to educate consumers about commercial data privacy practices.

III. Internet of Things Best Practices Privacy Framework

The Federal Trade Commission also issued an Internet of Things (IoT) privacy report in 2015 that sets forth "best practices" with respect to protecting consumer information in the particular context of the IoT. The IoT refers to the "ability of objects to connect to the Internet and to send and receive data." For the purposes of the FTC's framework, these objects may be devices or sensors (other than computers, smartphones, or tablets) that connect, communicate or transmit information with or between each other through the Internet and that are sold to or used by consumers (rather than in a business-to-business context). The IoT presents unique potential security risks as identified by the FTC, including enabling "unauthorized access and misuse of personal information," facilitating cyber-attacks, personal safety risks, and privacy issues arising from the monitoring or collection of "personal information such as habits, locations, and physical conditions over time."

See the FTC's IoT privacy report. The best practices articulated in the IoT privacy report include: (A) Security; (B) Data Minimization; and (C) Notice and Choice.

A. SECURITY

Companies should:

- build security into products at the outset, including:
  - conducting a privacy or security risk assessment
  - minimizing the data that is collected and retained
  - testing security measures before launching products.
- train company personnel on best security practices.

- retain service providers who are capable of maintaining reasonable security, and provide oversight for such providers.
- implement a "defense-in-depth approach" to identified significant risks within company systems.
- implement "reasonable access control measures" to limit unauthorized access to an IoT device, data or network.
- "monitor products throughout the life cycle and, to the extent feasible, patch known vulnerabilities."

B. DATA MINIMIZATION

1. Companies should consider reasonably limiting their collection and retention of consumer data in order to guard against the following two privacy-related risks:

- Large amounts of data stored present a more attractive target for malicious actors and increases potential harm to victims of an attack.
- Large amounts of data increase the risk that data will be used in a way that differs from consumers' reasonable expectations.

2. To accomplish data minimization, companies should implement one of the following options:

- abstain from collecting data altogether;
- collect only those fields of data necessary to the product or service;
- collect data that is less sensitive;
- de-identify (i.e., anonymize) collected data; or
- if none of the above options will fulfill the company's business goals, obtain consumer consent for collecting additional, unexpected categories of data

C. NOTICE AND CHOICE

1. Privacy choices offered by companies must be "clear and prominent"—not buried within lengthy documents.
2. Consumer choice ***must be offered*** when use of data would be inconsistent with the context of the interaction (i.e., an unexpected use).
3. By contrast, consumer choice ***would not be required*** in the following instances:
   - where use is consistent with the context (i.e., an expected use);
   - where collected data is "immediately and effectively" anonymized.
4. Recognizing the practical difficulty of providing choice when there is no consumer interface and that there is no one-size-fits-all approach, theFTC suggested the following options (which could be implemented in combination)forofferingnoticeandchoiceintheIoT sphere:
   - Develop video tutorials;
   - Affix QR codes on devices;
   - Provide choices at point of sale, within wizards or in a privacy dashboard

IV. Children's Online Privacy Protection Act

The Children's Online Privacy Protection Act, 15 U.S.C. § 6501 et seq. ("COPPA") and the associated implementing regulations, 16 C.F.R. Part 312 (the "COPPA Rule") impose obligations

on the operators of websites or online services (including mobile applications) that collect, use, or disclose (directly or indirectly) personal information from children under the age of 13. The COPPA Rule broadly defines "collection" to include the gathering of personal information by any means, including by:

- requesting or encouraging a child to submit personal information;
- "enabling a child to make personal information publicly available;" and
- "the passive tracking of a child online."

The COPPA Rule (16 CFR § 312.2) also broadly defines "personal information" to include:

- first and last name
- address
- online contact information (such as an e-mail address or other identifier that permits direct contact online)
- screen or user name permitting direct contact online
- telephone number
- social security number
- persistent identifier (such as IP address or device identifier) that can be used to recognize a user over time and across different websites
- photograph, video or audio file containing a child's image or voice
- geolocation information sufficient to identify a street name and name of city or town
- information concerning the child or parents that the operator collects online from the child and combines with any of the above

With the understanding that the COPPA regulations include detailed requirements with respect to each obligation, as a general matter, the obligations of a website or online service that is directed to children under COPPA include:

1. posting an online privacy policy describing the operator's practices with respect to children's information (16 CFR 312.4);
2. providing notice to parents before collecting, using, or disclosing information from children under 13 (16 CFR 312.4);
3. obtaining verifiable parental consent to the collection, use, or disclosure of information from children under 13 (16 CFR 312.5(a));
4. not conditioning a child's participation in an activity on the child disclosing more information than is reasonably necessary to participate (16 CFR 312.7);
5. honoring a parent's ongoing rights with respect to information collected from their child (i.e., allow a parent a means to review a child's personal information, to revoke their consent and refuse to permit further use/collection of personal information, and to delete their child's personal information) (16 CFR 312.5(b)(vi));
6. implementing reasonable procedures to protect the confidentiality, security, and disclosure of personal information collected from children, including by taking reasonable steps to release such information only to parties capable of maintaining its confidentiality and security (16 CFR 312.8); and
7. retaining personal information collected online from a child for only as long as is necessary to fulfill the purpose for which it was collected and delete the information using reasonable measures to protect against its unauthorized access or use (16 CFR 312.10);.

See the FTC's overview guide regarding COPPA compliance as well as a Frequently Asked Questions document.

V. Massachusetts Model for Data Protection Standards & FTC Data Security Guide

Massachusetts has enacted stringent data protection regulations (the Massachusetts Standards for the Protection of Personal Information of Residents of the Commonwealth, 201 C.M.R. 17.00 *et seq.*,) (the "Massachusetts regulations") and data disposal legislation (Mass. Gen. Laws ch. 93I).

Although the definition of "personal information" under the Massachusetts regulations is relatively narrow (a Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number), the Massachusetts regulations impose high minimum standards for protecting such information. ***Indeed, while other states may simply require the maintenance of "reasonable" safeguards to protect personal information of their residents, the Massachusetts regulations provide specific, granular detail as to the administrative, technical, and physical safeguards that must be maintained.***

Among other requirements, the Massachusetts regulations require the adoption of a written information security program (WISP) including certain minimum administrative, technical and physical safeguards – among which are to oversee third-party service providers and adhere to specific computer system security requirements. To assist in the compliance process, the Massachusetts Office of Consumer Affairs and Business Regulation has created a compliance checklist.

Similarly, although the recommendations are somewhat less granular than the requirements outlined in the Massachusetts regulations, the FTC has released a data security guide that culls the lessons learned from the FTC's 50+ data security enforcement actions into 10 recommendations.

In the absence of federal data security legislation, the FTC's data security guide – along with the Massachusetts data protection regulations, even in contexts where they are not applicable – can provide an effective starting point for a data protection strategy. Companies could even consider implementing the Massachusetts requirements with respect to ***all personal information*** it handles (not simply the narrow definition under the Massachusetts regulations).

VI. Breach Notification Requirements

Because there is no federal data breach notification law, in the event of a data breach, the required response actions vary on a state-by-state basis and frequently involve providing notice (including designated content) to specified state agencies as well as to the affected individuals. States also vary with respect to what constitutes a breach triggering notice requirements.

The Massachusetts security breach notification law is Massachusetts General Laws Ch. 93H and the Massachusetts Attorney General's guidance with respect to security breaches is available here.

Note that insurance coverage may be available to address liability associated with data breach (including indemnity/regulatory coverage) as well as breach response (including call center establishment and notification). See, *e.g.*, the cybersecurity statement of the National Association of Insurance Commissioners.

VII. SEC Cybersecurity Guidance

The U.S. Securities and Exchange Commission is increasingly concerned about the risk that cyber attacks pose to public companies and has initiated efforts to assess cybersecurity preparedness in the securities industry. In 2016, cybersecurity continues to be included in the SEC's Office of Compliance Inspections and Examinations (OCIE) priorities list. OCIE released Risk Alerts in April 2014 and September 2015, and the respective Appendix to each contains a sample list of requests for information that the OCIE might use in conducting examinations of registered entities regarding cybersecurity matters. These sample lists may be useful for all businesses (whether or not they are regulated by the SEC) in identifying and addressing cybersecurity risks. See the sample lists (and associated Risk Alerts).

* * * * *

VIII. Triggers for Privacy/Data Security Concerns and Potential Action Items

To assist companies in navigating the U.S. privacy and data security landscape, we have developed the following list of triggers, which may indicate the presence of privacy-related legal issues and which should prompt consultation with privacy counsel:

- **Handling any of the following classes of information:**
  - – Medical/Health
  - – Credit/Debit Card or Bank/Financial Account
  - – Social Security Numbers
  - – "Personal Information" within the meaning of the Massachusetts regulations (described above)
- **A business with any online presence and particularly those which:**
  - – Feature any advertising
  - – Are directed to or are appealing to children or minors
  - – Are used primarily for K-12 school purposes
  - – Provide technology services relating to K-12 students
- **Knowledge or suspicion of a security breach**
- **Engaging in certain actions, including:**
  - – Corporate merger or acquisition transactions
  - – Transfer of data to/from international locations
  - – A third party service arrangement pursuant to which a service provider may receive, or a service recipient may share, data (including customer data)
- **Not having a privacy policy or having an outdated privacy policy**

- **Not auditing information collection and handling practices to ensure compliance with your stated privacy policy and any applicable laws**

As to potential action items, we recommend considering the above list of triggers, consulting with counsel, and collaborating on the following steps:

- Assess privacy practices to determine areas of weakness and strength within your company and accordingly initiate a best practices approach going forward that is particular to your business model.

- Based on the results of this assessment, adopt (or revise, as needed, any existing) documentation of the company's privacy and data security practices; distribute the same internally within your employee base for ongoing reference and compliance and, to the extent required, make available online or in other necessary contexts.

- Conduct annual assessments of the company's compliance with its stated privacy and data security practices and make adjustments and improvements as needed.

To discuss your specific privacy and data security legal services needs, please contact **Faith D. Kasparian**, **Amanda Schreyer**, **Michael J. Cavaretta**, or **Howard G. Zaharoff**.

The author would like to acknowledge the contributions to this article by, and give thanks to, Leslie Bitman, Senior Librarian.