CLIENT ALERT

Business Transitions and Personal Information: Managing Privacy Risks

June 2015

The mantra for managing privacy risks—think privacy throughout the information life cycle—is embedded in Fair Information Practice Principles, Privacy by Design principles, Federal Trade Commission (FTC) and other federal and state privacy guidance and enforcement activities, privacy self-regulation programs, and private consumer protection litigation. Although each organization might use slightly different terms to describe its information life cycle—for example, collection, storage, use, disclosure, retention, and disposal—the more actively organizations anticipate and address actual and potential privacy (and other) risks associated with each component of their information life cycle, the stronger their overall risk management program becomes.

Privacy risks can be particularly high when organizations have not planned for the possibility that personal information will need to be used, disclosed, retained, or disposed of in circumstances other than day-to-day business operations. As demonstrated by two recent examples, business transitions can be one such circumstance, whether as a changed organizational structure or mission, such as a merger or acquisition or reinvention, in which personal information might be transferred, combined with information from other sources, or used for additional or different purposes; or as a bankruptcy, in which customer information might be a valuable and saleable asset of the estate and thus of interest to parties who have no relationship to the individuals from whom that information was collected.

Consistent with its strong support for the role of notice and choice in the collection and use of personal information, the FTC may intervene to raise privacy issues in business transitions if it is concerned that previously collected personal information might be used inconsistently with the privacy representations made at the time of collection or that the privacy representations will subsequently be changed and applied to previously collected information without providing consumers with prior notice and meaningful options. Those same concerns can also attract the attention of other regulators, consumer advocates, privacy watchdogs, media, and others, and thereby increase the risk that privacy-related aspects of a business transition will lead to collateral actions such as federal and state consumer protection enforcement actions and, potentially, private litigation.

Changes in Business Structure or Mission

When Facebook, already under FTC order for prior privacy-related conduct, acquired the instant messaging service What's App, FTC staff sent a letter to both companies. The FTC reminded each entity that they "would continue to be bound" by What's App's original privacy representations, which significantly limited the collection and use of personal information; that any subsequent changes in use of previously collected personal information required prior consumer consent; and that any privacy-related failures to properly handle What's App personal information could violate the prior FTC order. The FTC also recommended that any future privacy-related changes affecting newly collected information include an opportunity for users to either opt out of the changes or stop using What's App.

Bankruptcy

As widely reported in the media, one of the significant assets in Radio Shack's bankruptcy estate was a database of customer information, estimated to contain up to 117 million individual records. Radio Shack's privacy representations to customers, like What's App's to its users, included the absolute representations often found in privacy policies: "We will not sell or rent your personally identifiable information to anyone at any time" and "We pride ourselves on not selling our private mailing list." This restrictive language, coupled with the high level of media and other interest in the potential sale of that personal information, triggered the bankruptcy court's appointment of a consumer privacy ombudsman, a new role created in the 2005 amendments to the Bankruptcy Code, 11 U.S.C. §§ 323, 362.

The consumer privacy ombudsman had to make a recommendation to the bankruptcy court to resolve a number of privacy-related issues, including objections from

- Attorneys General from Texas and 38 other states on the grounds that Radio Shack's privacy representations to consumers absolutely prohibited sale of personal information without the advance express consent of affected consumers;
- Wireless carriers for whom Radio Shack sold equipment and data plan enrollments to customers on the grounds that personal information collected in connection with wireless service belonged by contract to the carriers, not to Radio Shack; and
- FTC staff, who in a May 16 letter to the consumer privacy ombudsman noted that "a sale or transfer of the personal information . . . would contravene Radio Shack's express promise not to sell or rent such data and could constitute a deceptive or unfair practice under Section 5 of the FTC Act." However, as in its past interventions in similar proceedings, the FTC also recognized that bankruptcy raises additional considerations and recommended specific sale-related conditions to protect customer privacy, including prohibiting a standalone sale of personal information, only selling personal information to a buyer engaged in a similar line of business who agrees to comply with RadioShack's privacy policy, and requiring the buyer to agree to obtain consumer consent before making any material changes in use of previously collected personal information.

To further complicate matters, the consumer privacy ombudsman determined that Radio Shack had aggregated the personal information it collected across its business activities and locations and thus that personal information could not be segregated based on source, business activity, or point of origin and that the accuracy and completeness of the information could not be determined. Ultimately, the consumer privacy ombudsman used mediation to address specific issues and recommended sale of the personal information on terms consistent with the FTC recommendations and with terms used by consumer privacy ombudsmen in prior bankruptcy matters. The bankruptcy court accepted the recommendation and permitted sale of a limited amount of personal information to an entity that plans to continue business operations.

Takeaway

The challenge for any organization that handles personal information—and today that is virtually every organization—is to harmonize the tension between the business value of working with personal information; the privacy (and other) risks associated with collecting, storing, using, disclosing, retaining, and disposing of personal information; applicable legal

requirements; and the organization's tolerance of risk. In other words, a comprehensive, organization-wide risk management program that addresses privacy, data security, compliance, and other considerations.

In terms of anticipating and, to the extent possible, addressing privacy-related issues associated with business transition scenarios, risk management considerations should include:

- Knowing what personal information the organization collects and what privacy representations were made to individuals when that information is collected;
- Before acquiring personal information from third parties (whether from business partners acting on the organization's behalf or from an entity that compiles and sells personal information), reviewing the third party's privacy and collection policies and practices and knowing what privacy representations were made to the individuals about permissible uses of that information
- Creating policies within the organization to identify and appropriately handle personal information that needs to remain segregated because of source, representations made at the time of collection, nature of the information, legal and contractual obligations, or other considerations;
- Making sure that third parties handling personal information on behalf of the organization comply with the organization’s expectations and legal requirements, including by making sure that contract and other documents spell out rights and responsibilities with regard to data ownership, information security, collection, segregation of data, acceptable use, retention, disposal, subcontractors, training, and audit and enforcement rights. Don't forget to address what happens when things *don't* proceed as anticipated, including data incidents, bankruptcy, contract termination by either party, and acquisition or merger.
- When drafting privacy policies and providing pre-collection notice and choice to consumers, be mindful of the issues that can arise from strong representations about the limited use of personal information and consider including appropriate exceptions and qualifiers.
- Creating a process for reviewing and determining, in advance, whether changes in business practices or technology or collection and use of personal information pose new or increased privacy risks, including identifying who needs to be involved in that process and, if appropriate to the organization, what level of management needs to be involved in resolving different levels of potential privacy risks.
- Remembering that, from the FTC's perspective, a privacy representation made to consumers at the time personal information is collected is binding and, with limited exceptions in bankruptcy proceedings, the FTC considers conduct that retroactively or unilaterally changes the privacy representations or uses collected personal information in ways that consumers wouldn't expect without seeking consent or giving consumers the opportunity to avoid the change to be actionable under the FTC Act.

Other Articles in this Month's Edition:

- Proposed Legislation to Create a Uniform Standard for 'Made in America' Labeling
- EU Court Finds That Food Label May Be Misleading Even If List of Ingredients Is Not
- Advertisers in the Ring – A Roundup of This Month's Competitor Advertising Challenges: Broad Performance Claims and Narrow Support

---

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Peter B. Miller, CIPP/G/US/E, CIPM, CIPT
Senior Counsel – Washington, D.C.
Phone: +1 202.624.2506
Email: pmiller@crowell.com