

Presented:
22nd Annual Technology Law Conference

May 21 – 22, 2009
Austin, Texas

Personal Information as an Asset and a Source of Risk

**Bart Huffman
Erin Fonté**

Bart W. Huffman
Privacy, Data Security and Information Law
Cox Smith Matthews Incorporated
112 E. Pecan Street, Suite 1800
San Antonio, TX 78205
bhuffman@coxsmith.com
210-554-5331
*Certified Information Privacy Professional

Erin F. Fonté
Privacy, Data Security and Information Law
Cox Smith Matthews Incorporated
111 Congress Avenue, Suite 2800
Austin, TX 78701
efonte@coxsmith.com
512-703-6318
*Certified Information Privacy Professional

1. The Concept of Data Ownership

Outside of the traditional intellectual property framework, the notion of data ownership is multifaceted. From the perspective of identity theft statutes and the like, the data “owner” is the data subject. *See e.g.*, 15 U.S.C. § 1681c(g) (provision of Fair and Accurate Credit Transaction Act (“FACTA”) requiring truncation of credit card and debit card numbers on receipts provided to cardholders); TEX. BUS. & COM. CODE § 48.101(a) (provision of Texas data breach law prohibiting possession, transfer or use of personal identifying information of another person without such person’s consent and with harmful intent). Beyond that, custodians or holders of data can be thought of as data controllers or data processors. Under European Union (“EU”) law, for example, data controllers are organizations that have the authority to control how and for what purposes data may be processed, while data processors are organizations that process (store, manipulate, use, delete) data on behalf of the controller. *See* Council Directive 95/46, Ch. I, arts. 2(d) and 2(e) (EC).

As used in this paper, the terms “data controller” and “data processor” refer generally to primary holders and users of data and secondary holders and users of data, respectively (and not to the technical definition of those terms under EU or other law). For example, a retailer would be a “data controller” for the purposes of this paper with respect to customer details and associated purchase history. That retailer may utilize the services of third-party marketing, payment card, shipping, and other service providers, all of whom may require access to some of the customer data in order to provide the services, and all of whom would be “data processors” for the purposes of this paper.

Generally speaking, the permissible uses of data by a data controller are set by the data controller’s privacy policies and applicable law, while the permissible uses of data by a data processor are set by the data controller (as well as applicable law). Thus, as between the two, the data controller has more “power” over the data, and is more akin to a data “owner.”

As will be further addressed herein, data “ownership” is a function of attributes such as the associated power, control, and ability to use to use the data.

2. Data and Privacy Value

Obviously, in the “information age,” information has substantial value. Thus, a combination of personal data (concerning customers, subscribers, leads, etc.) plus the ability to use that data can be critical for ongoing operations (such as support functions, communications, and providing the actual service requested by a customer). But such a combination is also regularly and extensively used to generate direct sales and advertising revenue, and may even be sold outright.¹

¹ Data lists can be purchased from companies such as Experian Information Solutions, Inc. Recently, consistent with the trend towards customizing (and monetizing) data, companies such as BlueKai, Inc., sometimes referred to as “behavioral exchanges,” sell purchase history data and the like to interested companies, ostensibly with consumer consent and some level of customer control, for highly-targeted marketing purposes. *See* John Cook, *BlueKai Gets \$10.5 Million to Help Advertisers Target Shoppers*, Techflash, Dec. 15, 2008, http://www.techflash.com/BlueKai_gets_105_million_to_help_advertisers_target_shoppers36189094.html (last visited Apr. 23, 2009).

Importantly, although the type and amount of data a company holds may be fairly easily determined, it is considerably more difficult to determine the constraints on the ability to use that data. Both must be determined, though, in order to assess the data's value.

And it is not just the value of the data and the ability to use data that is significant. Increasingly, consumers and business customers pay careful attention to, and respond based on, their perception of the privacy policies and related security associated with the data they provide or generate. In addition, poor privacy practices can lead to enforcement actions, consumer lawsuits, or employee lawsuits. Aside from exposure issues, it is today an accepted, basic fact that customer retention requires the careful handling of customer data.² Simply put, a company's data privacy and security practices are increasingly important considerations in the assessment of a company's overall value.

As discussed further below, a number of risks, responsibilities, and limitations (collectively, and informally, referred to in this paper as "strings") may be attached to the personal data that a company possesses and uses as a data processor or a data controller. For the most part, a general assessment of a company's privacy and data security practices (and associated goodwill) will flow from examining these aspects of the personal data that the company possesses or uses. Nonetheless, any formal diligence should also cover past security breaches, complaints, lawsuits, and any regulatory inquiries with respect to a company's privacy practices.

3. Strings That May Be Attached to Personal Data

A. "Strings" for Data Controllers

The first privacy item any company that is a data controller must analyze is its customer-facing privacy policy. A privacy policy is, in effect, a contract between the company and the customer or other person providing his or her personal data (*i.e.*, the data subject). A privacy policy must remain in compliance with all applicable laws, and the company's practices must match the stated policy. Enforcement actions brought by the Federal Trade Commission ("FTC") clearly establish that the FTC views a company's privacy policy as a contract between the company and the customer. Violation of a stated privacy policy is treated as an unfair and deceptive trade practice under Section 5 of the FTC Act, 15 U.S.C. § 45(a). For example, if a privacy policy states "your information will never be shared with a third party," selling the data in bankruptcy would be a violation of the company's privacy policy, and an unfair and deceptive trade practice. *See., e.g., Federal Trade Comm'n v. Toysmart.com, LLC*, 2000 WL 34016434 (D. Mass. July 21, 2000).

Importantly, the applicable privacy policy is the one in existence when personal data is collected. Data controllers must anticipate future needs regarding data collection, use and sharing, and revise their privacy policy accordingly to encompass future activities, including merger, sale, acquisition and even bankruptcy, liquidation or dissolution. Privacy policy amendments do not

² In some areas, a solid privacy and data security reputation is an influential factor in the customer's initial decision whether to do business with a company.

apply retroactively, *see., e.g., In re Gateway Learning Corp.*, FTC, File No. 042-3047 (settlement July 7, 2004), so a data controller that changes its privacy practices must generally obtain new customer consent in order to use personal data gathered under the old privacy policy in the new manner that differs from the prior version of the privacy policy. Again, careful analysis and drafting to encompass potential future uses can avoid the need to notify customers of changes and obtain additional consent.

Data transfer laws in certain jurisdictions (*e.g.* the EU) may limit a company's ability to transfer personal data out of that jurisdiction without complying with applicable privacy laws. Transfers of employee or customer personal data, even within a company operating in multiple countries, may be affected. Such data transfer and privacy laws apply to the data controller's transfer actions, but could also apply to actions taken by certain third party vendors or other data processors, such as a cloud computing service provider that stores personal data for others and moves it across national borders to various service centers located in various countries.

A data controller should also remember that personal data physically located within a jurisdiction may become subject to governmental or private discovery in that jurisdiction. If a company does not already know in which jurisdictions its personal data physically resides, it should take steps to find out so it can ascertain which national privacy (and other) laws may apply.

A company accepting credit cards or debit cards for payment is subject to Payment Card Industry Data Security Standards ("PCI-DSS") requirements regarding payment and transaction data. The PCI-DSS standards are enforced via private contract by payment card associations (*e.g.*, Visa and MasterCard) and prohibit the retention of certain transaction data. States have also enacted laws imposing liability on companies that improperly retain certain transaction information, including personal cardholder data. Data controllers must meet PCI-DSS requirements to avoid potential fines and penalties from payment card associations, and to comply with applicable state laws. Data controllers must also assess their payment systems procedures, equipment, and other systems (including point-of-sale terminals) for compliance with the federal FACTA card account number truncation and expiration date suppression requirements, as well as various similar state laws applying to cardholder transaction receipts.

For any data controller that sends commercial email, there is an ongoing obligation to maintain and utilize internal suppression lists, in accordance with federal CAN-SPAM (and state law equivalents), and perhaps other applicable marketing laws. The company also must abide by any national "do not call" or "do not text" registries that may be in effect in applicable jurisdictions.

Forty-four states, the District of Columbia, Puerto Rico and New York City have enacted data breach notification laws. There are a number of issues a data controller must face to comply with various state laws after a data security breach involving personal information. However, under a majority of state data breach notification laws, a data controller only has a duty to notify affected individuals if the data breach involves unauthorized acquisition of unencrypted data. If personal data is encrypted, the company faces significantly reduced notification obligations under current state laws. When investigating data breach incidents, the FTC has examined

whether a company's security and encryption practices (a) meet the stated privacy policy and (b) are commercially reasonable. It is considered commercially unreasonable for a company not to have data security policies in place regarding personal data. In Massachusetts, the state's Office of Consumer Affairs & Business Regulation adopted regulations (effective January 1, 2010), requiring any company that owns, licenses, stores or maintains personal data about a Massachusetts resident (employee or customer) to follow certain mandatory encryption, data security and other technical requirements. *See* 201 MASS. CODE REGS. § 17.00 *et seq.* *See also* NEV. REV. STAT. § 597.970 (similar law regarding encryption of Nevada resident and customer information). Several other states are considering the adoption of similar measures.

Legal responsibilities for personal data run throughout the full "life cycle" of the personal data: data creation/collection, use, transfer, sale and ultimately, destruction or disposal. Data controllers should be aware of laws regarding proper disposal of personal data. For example, the FTC Disposal Rule (promulgated under FACTA), 16 C.F.R. § 682, requires any maker, user or custodian of a credit report to dispose of the report "properly," which generally means employing "reasonable" disposal measures that render the personal data unreadable or incapable of being reconstructed. The Texas document disposal and destruction law requires Texas businesses to dispose of business records containing personal data by modifying, shredding, erasing, or otherwise rendering the records unreadable or indecipherable.³ *See* Texas Information Disposal Act, TEX. BUS. & COMM. CODE § 35.48. Fifteen other states also have data security and destruction laws addressing documents containing personal data.

Data controllers are also generally responsible for their third-party vendors' actions. The conduct of such vendors is, in turn, subject to laws of jurisdictions where data is stored or processed. In some industry-specific areas, such as financial services and healthcare, data controllers have government-imposed responsibility for the actions of third-party vendors with respect to personal data. All data controllers should conduct diligence on their vendors that includes asking questions about the actual and potential physical location of personal data, general security information surrounding storage and transfer of such data, and any industry-specific questions that may be appropriate. For example, bank vendors must now demonstrate compliance with the new Identity Theft Red Flags Rules to their banking clients.

Data controllers should also conduct due diligence regarding personal data they acquire from third-party vendors, such as marketing lists. In one notable case, a Florida-based telemarketing company bought customer leads containing personal data stolen from Certegy in a prior, highly publicized data breach. The Certegy breach victims contacted the Florida Attorney General after they were contacted by the telemarketer. On April 8, 2009, the company entered into a settlement with the Florida Attorney General (and paid \$350,000 in penalties) for alleged violation of Florida's unfair and deceptive trade practices act arising from the company's complete lack of due diligence in determining whether the data purchased was of unlawful or even questionable origin. *Florida v. VICI Mktg., LLC*, No. 09-6303, Fla. Cir. Ct., *settlement approved* April 8, 2009. While currently an outlier case, it remains to be seen if other state

³ The Texas Attorney General has recently brought a number of actions alleging that companies are improperly disposing of business records containing personal data. *See, e.g.,* Agreed Final Judgment and Permanent Injunction, *State of Texas v. CVS Pharmacy, Inc.*, No. CV-72881, 253rd District, Liberty County, Texas (available at http://www.oag.state.tx.us/newspubs/releases/2008/032608cvs_afj.pdf).

attorneys general may follow suit, perhaps creating a new due diligence standard for acquisition of personal data.

In addition to the above, data controllers should be ever mindful of public perceptions and negative publicity that can arise from a data controller's privacy practices. Negative publicity regarding data breaches, such as the TJ Maxx and Heartland Payment Systems breaches, illustrate how companies can invoke negative public opinion not just because of the data breach itself, but also due to their subsequent handling (or mishandling) of the breach. Recent outcry over the proposed changes to the Facebook terms of use is an example of how public opinion can turn negative if customers or users believe their expectations regarding privacy and use of personal data are suddenly changed unfairly and unilaterally by the company.

B. "Strings" For Data Processors

Many if not most of the above items that constitute "strings" for data controllers are also "strings" for data processors, but data processors may have unique responsibilities and other concerns. For example, although a data controller's privacy policy should continue to apply when the data processor is handling the data controller's data, a data processor's own privacy policy may apply when conducting certain online activities where the data processor's client pushes its customers to the data processor's own website.

Today's business customers (the data controllers) increasingly expect very high standards and clarity from their data processor vendors with respect to data privacy and security measures. Data processors should understand that such measures are a critical part of their business reputation and ability to attract and retain business. Some data controllers may even engage in "compliance outsourcing," wherein the data processor is hired, in part, to assume legal responsibility for specific areas of privacy law compliance, such as maintenance of data suppression lists and compliance with government "do not contact" registries.

Data processors, particularly those who take on more traditional "in house" functions, should be aware that data controllers are asking for more detailed information regarding data security, physical location of data and compliance with applicable laws. While the data controller may give up either temporary or permanent possession of personal data, the data controller is still generally responsible for compliance with privacy laws and therefore must "deputize" the data processor, the possessor of the personal data, into a compliance role.