FUNKHOUSER VEGOSEN LIEBMAN & DUNN LTD.

Legal Update

June 2015

DATA PRIVACY: KNOW AND ADDRESS THE RISK BEFORE IT'S TOO LATE

By Peter T. Berk

Data privacy looms large in the law and in the news today, and corporate leaders need to be aware of their risks. There are numerous State statutes, as well as Federal laws (including HIPAA and the Americans with Disabilities Act) and regulations that are implicated in this area. Companies that experience data breaches face expenditures to discover the cause of the breach and restore security, as well as to make notifications required under the various State laws, not to mention obvious public relations issues. Additionally, these companies may also have to contend with regulatory investigations and fines, State Attorneys General actions and investigations, class action lawsuits, monetary damages, and the cost of fraud monitoring for a number of years for those whose data was stolen. Given these risks, it is imperative that companies invest the appropriate resources to ensure that they are taking the necessary steps to best protect themselves from potential breaches. Below is a sample of six areas that companies tend to either overlook or not fully investigate when dealing with data privacy:

1. Be Aware Of The Customer Data You Collect

Companies often don't realize how much, or what type, of data they collect about their customers. Companies obviously have customer data from purchases and payments, such as name, address, and credit card information. Companies, however, usually desire to, and do, have more connections with their customers and clients. For example, a company's internal marketing database (including a customer loyalty program) can hold names, addresses, email addresses and birthdate information. Likewise, customer service/complaint records – which can include recordings of customer calls as well as large databases – can reveal customer names, telephone numbers, addresses, and credit card information. Interactive website features, such as member's areas, chatrooms, and on-line help sessions can record, log, and track a large amount of data, even if not directly offered by the customer. When considering data privacy issues and risks, the first step is always to understand what data your company collects, where it is located, and where it is used within the organization so that your company can make informed decisions about what it needs to keep or collect, and how to protect the data it does keep.

2. Be Aware Of Other Personal Data Collected

Often, companies are very focused on their customers, as well they should be. But when considering data, companies cannot overlook their employees. Companies capture and retain large amounts of personal identification information, and in some cases even health information, about their employees. Simply because an individual is an employee does not make his or her data less worthy of protection.

Companies maintain the obvious types of data about their employees such as names, addresses, phone numbers, and birthdates. But companies usually also have social security numbers, bank account information (e.g., for direct deposit of paychecks), and, in some cases, health history and current health status (especially if the company administers its own health insurance or wellness program).

3. Pay Attention To Vendor Contracts

Because data privacy is a big issue, and the exposure for a breach potentially reaches into the millions of dollars, assessing who bears the risk for a breach is becoming a large part of vendor contract negotiation. Usually one or both parties try to include clauses in contracts to shift the entire responsibility for data breach risk onto the other. Sometimes the request to shift the risk is based on what service the vendor is performing (such as installing a data security system), or who owns and uses the data collected. But many companies and vendors are putting boilerplate "hold harmless" and "indemnity" clauses for data breach into their standard contracts regardless of the circumstances. Many times the success of a contracting party's risk shifting depends on leverage in the relationship. That, however, does not mean that your company should ignore the wording contained in these clauses. Even if such a clause is proposed, it can, at times, be negotiated. Further, and in any event, if such a clause exists in a contract, your company must understand the terms and its potential liability, and plan for how it can try to limit the risk.

4. Pay Attention To Vendor Access

After a vendor is hired and the contract issues are dealt with, there is more to be done. While companies generally take actions to protect data from inadvertent (or even purposeful) loss or dissemination by employees, companies must be aware of the access they give vendors to the company's data and the systems holding that data. One need look no further than to the data breach that Target experienced, in which Target's data was accessed through stolen credentials from an HVAC contractor. Your company should be aware of the access it gives to vendors, consider how much, if any, access is necessary, and govern permissions accordingly.

5. Update Your Company's Privacy Policy

Virtually every company's website has a "Privacy Policy." But when was the last time it was reviewed and updated it? A lot may have changed in the law, or your company's practices, that make your company's policy outdated and inaccurate. There are State statutes that make misrepresentations in web privacy policies an enumerated violation of the State's Consumer Fraud Act. Further, some State Attorneys General are beginning to look at company privacy policies to ensure they (a) comply with the State's law, (b) make full and proper disclosure, (c) are accurate as to the information collected, and (d) are accurate as to what is done with the information (by the company or even third-parties with plug-ins on the company website).

6. Be Mindful Of Foreign Law

Everyone recognizes that the economy is no longer national but international. As a result, many companies are expanding their operations – through mergers, acquisitions, or organic growth – to other countries and customers, especially in European markets. When doing this, companies need to be

aware of the differing privacy laws and standards (e.g., Europe's "right to be forgotten") that exist (and are constantly in flux) in foreign countries. What may be acceptable in the United States does not necessarily comply with the law elsewhere. Moreover, there are additional considerations and risks when data regarding individuals is transmitted internationally through electronic means. These considerations not only relate to laws of the various countries involved, but also the security of the transfer and whether it meets required standards. Consequently, companies expanding into foreign markets must consider whether or not to share individually identifiable data across international borders and, if so, how it will be handled.

While this is not, and is not intended to be, an exhaustive list of every data privacy issue that exists, the most important thing is for companies to address, and continually update, their data privacy risk profile. The issue of data privacy is front and center in customers' – as well as criminals' – minds. Ignoring it will work only until the company suffers a data breach.
