June 2011

MAYER·BROWN

Electronic Discovery & Records Management

Tip of the Month

E-Discovery and Data Privacy in the US

Scenario

An online retailer collects personally identifiable and private information about its customers, including their names, addresses, email addresses, cell phone numbers, birthdates, credit card information and "rewards points" account numbers for hotels and airlines. The retailer recently received a document request for "all information collected about each of your customers." The retailer's General Counsel is concerned not only about whether some or all of the information will be required to be produced, but also about how to protect the privacy rights of its customers in the event that production of the personal information is ordered.

Data Privacy and Discovery

Data privacy is one of the most hotly debated topics in both legal and business circles in the United States. Increasing cyber-attacks and high-profile data breaches have brought attention to the risks associated with a failure to protect the personally identifiable information of an organization's customers and employees. While references to data privacy and data protection often bring to mind the highly developed data protection laws in the European Union, there are numerous data privacy laws in the United States that affect the way organizations do business, including:

- Gramm-Leach-Bliley Act (GLBA)
- Right to Financial Privacy Act (RFPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Health Information Technology for Economic & Clinical Health (HITECH) Act
- Children's Online Protection Act (COPA)
- Payment Card Industry Data Security Standards (PCI DSS)
- State Breach Notification Laws
- State Data Transfer Laws

However, while many organizations employ privacy professionals, and are aware of their data privacy obligations in their day-to-day business operations, personally identifiable information that is collected in response to a document request often falls into the "black hole" of litigation. That is, once that data is collected for litigation, the organization stops scrutinizing whether the steps being taken to protect against data breaches or unnecessary disclosure are sufficient to meet the organization's legal obligations and minimize the risk of data breaches. While many organizations have policies and procedures protecting the private data of employees and customers in their

every day business activities, those same organizations often overlook the importance of applying those polices and procedures to e-discovery.

Given the emphasis on disclosure in US litigation and the frequent lack of coordination between data privacy professionals and in-house and outside counsel, the management of personally identifiable information in litigation represents a key area of risk. It is important for organizations and their counsel to recognize that there *are* risks associated with inadvertent disclosure and/or data breaches in the course of discovery. For example:

- In-house counsel will often apply the same over-collection philosophy to both non-private and private data.
- Data may be transferred to outside counsel or e-discovery vendors without proper data security measures.
- Organizations frequently fail to scrutinize their e-discovery vendors to ensure that those vendors are providing the same security protections that the organization itself is required to apply.
- Organizations often enter into (or permit their outside counsel to enter into) contracts with e-discovery vendors that do not contain sufficient protections against potential data breaches.
- Outside counsel may not apply the same level of scrutiny to protect personally identifiable information as is applied to privileged or other protected data.

There are ways to manage and mitigate the risks of data breaches associated with litigation. Considering data privacy issues at the outset of the discovery process can help limit the burdens and also minimize risks of producing private data.

Reducing Risks Through the Information Life Cycle

In-house and outside counsel should consider how to limit the transfer of private data and reduce the risk of a security breach at each stage of the information life cycle in the discovery process, e.g., collection, processing and production. For example, can the collection of personally identifiable information be limited at the outset of the litigation? Can the dissemination of that information be limited through confidentiality agreements and limits on third-party disclosure? If private data will be stored until the matter is finally resolved, what steps are necessary to ensure that the data is maintained securely? And, what procedures are necessary to ensure that any personally identifiable information is securely transferred?

Best Practices

- *Understand where protected information resides.* It is important to assess what personal data your business collects and uses, what privacy laws apply to that data and what your current practices may be with respect to the use and sharing of that data. To accomplish all this, many businesses employ privacy professionals or otherwise appoint a privacy team comprised of individuals from human resources, legal, marketing, communications, technology, finance, strategy and other departments. When litigation commences, litigators can confer with such privacy staff to understand what types of information are collected in the course of business that are subject to privacy protection.
- *Leverage existing resources.* A business' privacy group typically has controls in place to manage private data. Litigators can consider applying these existing procedures to manage such data in the course of discovery.
- *Negotiate what should be collected and produced.* Negotiating the scope of data to be collected and produced with opposing counsel at the outset can help to reduce the amount

of unnecessary and non-responsive data collected. It may also help to have candid discussions with opposing counsel regarding the scope of their requests. The requesting party may not realize they are asking for highly confidential information, and they may not want to be in possession of such information and expose themselves to the risks of a data breach. For example, the requesting party may want customer names and addresses, but not need customer birthdates or credit card information.

- *Organize data.* It is helpful to organize collected data so that segments containing private information can be targeted by the document review team and treated more efficiently.
- *Protect private data that must be produced in discovery*. The litigation may require that confidential and private information be produced. In such cases, it is common for the parties to enter into confidentiality agreements that dictate how this information will be treated. Pursuant to Rule 26(c) of the Federal Rules of Civil Procedure, a party may seek a protective order providing that confidential information may not be revealed or that it must be used in a limited manner (e.g., for attorneys eyes only).
- *Ensure vendors are protecting private data.* Private data can be most vulnerable to security breach when it leaves the business. Thus, when e-discovery vendors are used to process data in litigation, consider security safeguards including transferring only encrypted data, ensuring that the vendor has sufficient security and privacy protocols, and limiting access to the data by the vendor's staff.

Protecting private data is the responsibility of both in-house and outside counsel. Knowing where private data is kept, leveraging your business' existing resources for managing such data, negotiating the scope of production and having policies and procedures to protect that data will limit the risks of inadvertent loss when production is required.

For inquiries related to this Tip of the Month, please contact Kim A. Leffert at kleffert@mayerbrown.com, Seema V. Dargar at sdargar@mayerbrown.com, or Michael Lackey at mlackey@mayerbrown.com.

Learn more about Mayer Brown's Electronic Discovery & Records Management practice or contact Anthony J. Diana at adiana@mayerbrown.com, Michael E. Lackey, Jr. at mlackey@mayerbrown.com or Ed Sautter at esautter@mayerbrown.com.

Please visit us at www.mayerbrown.com

Mayer Brown LLP, 71 S. Wacker Drive, Chicago Il, 60606, Tel: +1 312 782 0600