Privacy and Data Security: Breach Notification

This Note provides practical tips on how to prepare for and respond to a data security breach and explains certain US federal and state data breach notification laws relating to personal information.

Lynda K. Marshall and Timothy P. Tobin, Hogan & Hartson LLP

According to the Chronology of Data Breaches by the Privacy Rights Clearinghouse, since the beginning of 2005, over 340 million records of individuals have been compromised in hundreds of known data breaches in the US. Data breaches happen for many different reasons, including due to:

- Human error and accidents, such as losing a computer or data storage device.
- The illegal or malicious activity of individuals and criminal enterprises (whether employees or other insiders or unrelated third parties) through hacking into an organization's computer system, obtaining information by pretext or phishing, or theft of equipment.

The cost of a data breach to businesses can be significant in terms of both expense and reputation, including the actual cost of responding to the breach, lost business revenue and exposure to government fines and penalties as well as private lawsuits. Because of the many threats and the significant costs, no matter how robust a company's data security practices and policies, there is no way to ensure that a data breach will not occur. Accordingly, companies should prepare for a data breach and develop a response plan that complies with legal obligations and reflects operational realities (see below *Preparing for and Responding to a Data Security Breach*). The response plan should specify each step to take once a breach is suspected, including identification of individuals responsible for each task. Regardless of the cause of a breach, having a plan in place will help ensure an appropriate response to avoid or minimize legal exposure and any public relations crises.

This Note considers key issues relating to:

- Preparing for and responding to a data security breach.
- State data breach notification laws.
- Federal data breach notification laws.
- Other state and federal data security laws.

PREPARING FOR AND RESPONDING TO A DATA SECURITY BREACH

PREPARING FOR A DATA SECURITY BREACH

Companies should have a plan in place to respond to a data security breach before a breach occurs. The plan should include, at a minimum:

- Setting up a standing security breach response team. Individual members of the team will vary, depending on the specific breach that arises, but should include representatives from:
  - the Office of General Counsel;
  - the Data Office;
  - Corporate Security;
  - Information Security;
  - Human Resources;
  - Internal Audits; and
  - Public Communication/Media Relations.
- Developing and implementing a written data security response plan setting out procedures in the event of a data security breach. The

plan should specify each step to be taken once a breach is suspected, including identification of individuals responsible for each task. As part of the written plan, the company should also consider developing procedures for:

- investigating a data breach incident;
- identifying affected individuals and obtaining contact information if not already available;
- providing notification to affected individuals where appropriate (see below *Developing a Notification Plan for Affected Individuals*); and
- responding to third party inquiries (see below *Designing an Inquiry Response Plan*).

WHAT IS THE FIRST THING TO DO WHEN A BREACH ACTUALLY HAPPENS?

If your organization experiences a data breach, it should begin immediate mitigation and incident analysis. This consists of five primary steps:

- Contain the data security breach. As soon as the company becomes aware of a data breach, it should take all necessary steps to investigate the incident promptly and limit further data loss. For example, if the breach involves data on company premises, the company should:
  - immediately secure the physical area housing the data (and change any locks, access codes or cards, as appropriate);
  - isolate all affected systems;
  - determine whether law enforcement should be notified; and
  - determine whether traffic into the affected area should be limited until security officials or law enforcement authorities investigate.
- Convene a response team. Responding appropriately to a data breach requires coordination by multiple individuals across many company areas, and the company should have already in place a standing security breach response team (see above *Preparing for a Data Security Breach*).
- Collection of data related to the breach. When possible and at the direction of counsel, collect available data related to the breach (see *Box, Information to be Collected Immediately Following a Data Security Breach*). The company should as quickly as possible determine what business customer(s) are involved.
- Analyze the facts surrounding the breach. The company should evaluate and understand the root cause of the incident, including identifying:
  - who the affected persons are;
  - what personal information has been compromised;
  - what is likely to happen to the data that was compromised; and
  - whether other systems are under a threat of immediate or future danger.

  The company should consider seeking the assistance of specialized consultants in capturing relevant information and performing forensic analysis, especially if the scope of the breach is large or if it is difficult without such analysis to determine what business customers may be implicated. Time is of the essence as many state laws have time limits for notification.
- Analyze contract and legal implications of the breach. Legal analysis should include:
  - immediate analysis of the relevant business customer contracts for notification and other obligations, if applicable;

INFORMATION TO BE COLLECTED IMMEDIATELY FOLLOWING A DATA SECURITY BREACH

The information to be collected immediately following a data security breach includes:

- Date, time, duration and location of breach.
- How the breach was discovered, who discovered the breach and any known details surrounding the breach, for example:
  - method of intrusion;
  - entry or exit points;
  - paths taken;
  - compromised systems;
  - whether data was deleted, modified and/or viewed; and
  - whether any physical assets are missing.
- Details about the compromised data, including:
  - a list of affected individuals and type (for example, employee, vendor and customer);
  - data fields (including all fields of personal information maintained);
  - number of records affected;
  - whether any data was encrypted (if so, which fields); and
  - the customers or other individuals whose data may have been compromised.

- litigation risk;
- breach notification requirements (see *Box, Statutory Data Breach Notification Requirements*);
- insurance coverage;
- indemnification;
- law enforcement investigations; and
- employee liability.

The company should review any other relevant contracts of parties involved in the breach (for example, vendor contracts), as well as any related website privacy policies and even marketing materials to see if the company owes notification or other obligations to any third parties with respect to data breached or if third parties have obligations to the company relating to the breach (for example, indemnification). In-house counsel should determine whether to contact outside legal counsel for assistance. If the breach involves third parties (for example, service providers or business customers), it may be necessary to communicate and coordinate with those third parties and their counsel early and often.

- Contact law enforcement. Consult legal advisors before notifying law enforcement in order to determine the appropriate response to any law enforcement inquiry. If necessary, contact the appropriate local or federal law enforcement agencies to enable immediate deployment of investigative capabilities. Assign one member of the security breach response team the responsibility for interfacing with law enforcement agencies. Law enforcement authorities may require a delay in the notification to affected persons or release of public information if these activities would hamper law enforcement investigations. In addition, local or federal law enforcement authorities may want to conduct an investigation into the company's security systems and its response to the breach as a part of their investigation of the incident. Even if no state notification law applies and law enforcement authorities do not conduct an investigation, consider:
  - whether to file a police report for the incident (for example, for a stolen laptop or burglary on the premises); or
  - whether it nonetheless makes sense to contact the state attorneys general or regulators.

STATUTORY DATA BREACH NOTIFICATION REQUIREMENTS

Steps to comply with the statutory notification requirements following a data breach include:

- Identifying legal jurisdictions involved. Identify the states and countries potentially involved in the breach by determining the location of the customers, employees and systems affected by the breach. In the US, 45 states and Washington, D.C., the Virgin Islands and Puerto Rico have such laws, and there are now federal rules, including rules relating to financial and health information and vendors.
- Identifying statutes triggered. Identify federal, state, and international statutes and regulations potentially triggered or violated by the breach. Identify the following information within the triggered laws:
  - type of data: determine whether compromised personal information would trigger data breach notification laws. Generally, notification could be required where the compromised data is unencrypted and includes affected persons' first and last names plus one of the following: Social Security number, driver's license number, state identification number, credit card number or bank account information with password;
  - law enforcement and state agency notification requirement: determine whether law enforcement or state agencies **must** be notified by law;
  - notify credit agencies: determine whether credit reporting agencies **must** be notified by law; and
  - additional federal or foreign laws: determine the applicability of other legislation such as the Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA) and/or member state laws implementing the EU Data Protection Directive.

DESIGNING AN INQUIRY RESPONSE PLAN

A company may receive a significant volume of inquiries in the wake of a breach and ensuing individual notification efforts. Companies should consider designing a system for handling inquiries before the occurrence of a breach. System design should address the following issues:

- Selecting a mode of communication with the public (for example, a toll-free number or an e-mail address).
- Selecting a mode of communication with employees.
- Training and hiring customer service representatives to staff inquiry response (or outsourcing such activities) and preparing a script.
- Notifying credit reporting agencies prior to a large notification of affected persons (or as required by applicable law).

- Documenting inquiry responses.
- Preparing online Frequently Asked Questions (FAQs). FAQs can be a useful reference for affected individuals and can help to reduce the number of calls to a call center.
- Having a relationship with an appropriate public relations firm and other vendors before a breach occurs.

DEVELOPING A NOTIFICATION PLAN FOR AFFECTED INDIVIDUALS

When required or desirable, the company should develop a notification plan for affected persons based on legal requirements and the company's contracts with other parties. The fundamentals for this plan should be in place **before** a data breach occurs. If the company provides notice, affected persons should be notified as soon as possible, subject to specific legal requirements. The notification plan should address the following issues:

- Preparing a list of persons to be notified and determining the mode of communication (typically a letter) for delivering notice. In some cases, the applicable laws may not require notice, but the company may decide based on the facts and circumstances of a particular incident to provide notification. Additionally, regulations and prior contractual agreements between parties may require a certain mode of communication. The company should be careful to minimize the number of accidental notifications (that is, persons who are notified, but who do not fall within the groups of persons intended by the company to be notified).
- The specific content to include in the notice, which must comply with applicable laws (and contractual obligations) and should reflect appropriate public relations considerations. The content may include the following information:
  - description of what happened (unless limited by applicable law);
  - type of protected data involved;
  - actions to protect data from further unauthorized access;
  - what the company will do to assist affected persons;
  - what affected persons can do to assist themselves;
  - contact information for company inquiry response system (a toll-free number should be provided); and
  - contact information for local and federal government authorities.
- Developing model notice templates that are available if a data breach occurs and can be tailored to the particulars of the incident.
- Whether to offer certain remediation services to assist affected persons following a breach, even if not required by law, including:
  - credit monitoring services;
  - identity theft insurance;
  - identity theft help information packets; and
  - compensation for identity theft.
- Developing relationships with vendors providing remediation services in advance of any data breach.

ACTIONS TO TAKE AFTER RESPONDING TO INITIAL BREACH

Even after containing and analyzing a data breach, delivering notices and implementing a recipient inquiry response system, organizations should not consider the matter closed. Significant legal action may follow, but even if that does not happen, it is important to study the incident to assess the adequacy of the response to the data breach to determine if changes must be made to the data breach response program and to help assess organizational data security and potential weaknesses. After experiencing a data breach, a company should:

- Prepare for litigation. The company should consider litigation matters that may arise, including:
  - civil lawsuits instituted by affected persons against the company;
  - an investigation of the company or specific employees, its business customers or its own service providers by law enforcement authorities and regulatory agencies; and
  - indemnification claims against third parties in the event that third parties are at fault for a breach.
- Review information technology systems and physical security. The company should conduct follow-up analysis of the breach to determine root causes. It should review applicable access controls and procedures (both those in place before the breach and those put in place as the result of containment efforts) to ensure that weaknesses have been addressed and resolved.
- Assess operational controls. It is important to:
  - assess company operations to determine necessary revisions to data collection, retention, storage, and processing policies and procedures;
  - assess the need for additional employee training in data protection policies and processes; and
  - review agreements (both form agreements and executed agreements) and policies to determine whether any updates or modifications need to be made. This includes agreements with third parties that handle personal information, website privacy notices and terms of service, agreements with customers or other third parties, and employee handbooks and policies.

- Evaluate response. After the company responds to the breach, it should evaluate its response and implement changes or additional measures to eliminate vulnerability and improve effectiveness in preventing and responding to future breaches.

OVERVIEW OF STATE DATA BREACH NOTIFICATION LAWS

Currently, 45 states (the exceptions are Alabama, Kentucky, Mississippi, New Mexico and South Dakota) plus the District of Columbia, Puerto Rico and the US Virgin Islands, have adopted data breach notification laws applicable to private businesses. These data breach notification laws require businesses to take certain steps when a data breach involving the personal information of individuals occurs. Because California was the first state to adopt a data breach notification law, this Note focuses on California law and goes on to describe some of the key variations among state laws.

CALIFORNIA

The structure of California's breach notification law (*S.B. 1386*), which serves as the general template for other state laws, requires notification to affected individuals of an unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality or integrity of personal information held by any business (*Cal. Civ. Code § 1798.82(a) and (d)*). Good faith acquisition of personal information by an employee or agent of the business is not a breach under the law if the personal information is not used or subject to further unauthorized disclosure (*Cal. Civ. Code § 1798.82(d)*).

Definition of Personal Information

California's breach notification law defines "personal information" as an individual's first name or initial with last name and one or more of the following, if either element is unencrypted:

- Social Security number.
- Driver's license number or California Identification Card number.
- Account number, credit card or debit card number; in each case, in combination with any required security code, access code or password that would permit access to an individual's account.
- Medical information.
- Health insurance information.

(*Cal. Civ. Code § 1798.82(e).*)

Notification Requirements

Notification must occur "in the most expedient time possible and without unreasonable delay." Notification may be delayed if law enforcement determines notice will impede a criminal investigation. A non-data owner experiencing a breach of personal information (for example, a vendor), is required to notify the data owner "immediately following discovery" (*Cal. Civ. Code § 1798.82(b)*). Notice provided in writing satisfies California's law, although the law also allows either electronic notice or substitute notice if certain conditions are met.

OTHER STATES

While other state data breach laws are similar, any practitioner counseling a client that has experienced a data breach affecting individuals in multiple states must be aware of the numerous variations in the laws. Even subtle differences can be significant. Some key variations among state laws include:

- Risk of harm thresholds. 34 state laws include risk of harm thresholds, which typically require notification only if the breach poses, or is likely to pose, a significant risk of harm to the affected individuals.
- Definition of personal information. Some states have expanded the definition of "personal information" to include:
  - date of birth;
  - mother's maiden name;
  - biometric data;
  - DNA data;

THE DO'S AND DON'TS OF RESPONDING TO A DATA BREACH

DO:

- Have a written post-breach response plan ready and tested before a breach happens.
- Make sure people know what role they will play when a breach happens.
- Have a communications plan regarding the breach.
- Know what regulations, statutes and contracts cover your post-breach obligations.
- Take all necessary steps to prevent further exposure of data when a breach happens.
- Find out what happened as soon as possible and preserve the evidence.
- Involve technology and legal experts as needed.
- Have draft model notices ready to be customized depending on the facts.
- Have relationships with vendors who can assist with data breach response already in place before a data breach.
- Contact law enforcement, credit reporting agencies and your insurance carrier as needed.
- Keep regulators informed where required by law and where appropriate. If the regulators are surprised, they will not be happy.

DO NOT:

- Delay in providing notice unless required by law. The time deadlines are strict.
- Communicate with the public about the breach until you know the fundamental facts.
- Ignore your important business customers and partners. Keep them informed.
- Skimp in providing help to consumers. Their goodwill could forestall legal difficulties.
- Forget to update your post-breach response plan regularly.

- passport number;
- tribal identification numbers;
- taxpayer identification numbers;
- account numbers disassociated from passwords or pin numbers; and
- health and/or medical insurance information.

- Format of records. Six states have notice provisions that apply to breaches related to paper records in addition to computerized data.
- Content of notification letters. At least 11 states and Puerto Rico mandate the inclusion of specific content in notification letters. Some of these provisions conflict, which can create expense and administrative burdens for a company experiencing a large data breach. For example, while some states require that notices include a description of the breach incident, Massachusetts law specifies that the notice not include the nature of the breach.
- Notice to government or regulatory agencies. Many states also require notice to consumer reporting agencies, and at least 13 jurisdictions also require notice to the state attorney general or some other state agency.
- Timing of notification. Some states require notice to state authorities before notifying affected individuals. For example, Maryland requires notice to the Attorney General before notice to individuals and New Jersey requires notice to the State Police before notice to individuals. While most states require notice to individuals using some variation of California's rule, "in the most expedient time possible without unreasonable delay," only a handful of states include specific individual notification timeframes. For example, Florida, Ohio and Wisconsin require notice within 45 days, subject to law enforcement or internal system security needs. In Maine, if notification has been delayed because of a law enforcement investigation or law enforcement has been notified, once law enforcement determines that notification will not compromise a criminal investigation, it must be provided within seven business days from that point.

Many of these statutes require individual notice even where there is minimal risk to the individual, which, in addition to the administrative burden of providing notice, could lead to individuals ultimately ignoring the many notices they receive, possibly missing the one instance where it really matters. However, apart from the purpose of notifying individuals so that they can protect themselves from identity theft, the negative publicity and legal and regulatory exposure from state notification requirements may result in increased awareness by companies of their data security obligations.

Liability for Failure to Comply

The California statute includes a private right of action that allows individuals to sue for actual damages that might result from not receiving (timely) notice. Only a handful of other jurisdictions have included a statutory private right of action, including:

- Louisiana.
- Maryland.
- New Hampshire.
- New Jersey.
- North Carolina.
- South Carolina.
- Tennessee.
- Texas.
- Virginia.
- Washington, D.C.

Most other jurisdictions allow for enforcement by the state's attorney general or consumer protection agency, who typically can sue for civil or injunctive relief. Some states cross-reference to existing consumer protection authorities and penalties while a number of states specify fines and penalties when the state brings an action. For example:

- Arizona law provides that an entity that wilfully and knowingly fails to notify may be liable for a fine up to $10,000 per breach.
- Under Florida law, if an entity fails to provide notice within the specified 45-day time period, that entity can be fined (per breach, not per individual):
  - up to $1,000 per day, up to 30 days;
  - $50,000 each 30 days thereafter, up to 180 days; and
  - if there is no notification within 180 days, a fine up to $500,000.
- Indiana allows for a civil penalty of not more than $150,000.
- New York law states that for reckless violations, companies are subject to fines the greater of $5,000 or $10 per failed notifications, capped at $150,000.
- Oregon's statute provides for fines of up to $1,000 per violation up to $500,000 for any single breach.
- Texas provides for civil penalties of between $2,000 and $50,000 per violation.
- Virginia allows for civil penalties of up to $150,000 per breach.

Helping to ensure that all requisite notices are made and done in the proper format and timeframe in order to avoid liability is a crucial responsibility for in-house and outside counsel and involves consulting the laws of each state (as well as applicable federal laws) involved. A list of state security breach notification laws with links to the text of each law is maintained by the National Conference of State Legislatures (see *ncsl.org*).

OVERVIEW OF FEDERAL DATA BREACH NOTIFICATION LAWS

Many companies doing business in the US would welcome a single federal data breach notification law that would preempt the myriad state laws. To date, no such broad law has been passed by both houses of Congress despite several efforts over the past few years. Most recently, on December 8, 2009, the House of Representatives passed the Data

Accountability and Trust Act, which, if it becomes law, would require an entity experiencing a breach to notify affected individuals, unless it determines that there is no reasonable risk of identity theft, fraud or other unlawful conduct (which can be presumed if the data is properly encrypted or otherwise rendered in an electronic form unreadable or undecipherable). Organizations suffering breaches would also be required to provide consumer credit reports to affected individuals on a quarterly basis for two years.

However, US federal law already includes certain sectoral data breach notification requirements, for example:

- Financial Services Modernization Act of 1999, also known as the Gramm-Leach-Bliley Act (GLBA). GLBA regulates the privacy and data security practices of financial institutions. In 2005, the federal banking regulators, which include the Office of the Comptroller of the Currency, the Federal Reserve Board, the Federal Deposit Insurance Corporation and the Office of Thrift Supervision, issued Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice (Interagency Guidance). The Interagency Guidance requires financial institutions subject to these agencies' jurisdiction (but not other financial institutions) to develop and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems. These entities must investigate breaches when misuse of sensitive customer information has occurred or is reasonably possible, notify their functional regulator and provide consumer notice if warranted. Sensitive customer information includes a customer's name, address or telephone number, in conjunction with a Social Security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the customer's account. The Interagency Guidance is not limited to computerized data.
- Federal Communications Act of 1934. In 2007, the Federal Communications Commission passed a data breach notification rule under Section 222 of the Federal Communications Act of 1934 applicable to telecommunications companies and the customer phone records they handle. The rules require telecommunications companies, on experiencing a breach of covered phone records, to notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) within seven business days. Companies must then wait an additional seven business days before notifying the customers whose information was affected by the breach unless the USSS or FBI request further delay for individual notifications. However, if there is a risk of immediate harm to consumers, they must be notified sooner. Telecommunications companies must keep records pertaining to breaches for two years. The revised rules also strengthen safeguards on phone records.
- Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH Act). As part of the economic stimulus package signed into law on February 17, 2009, the HITECH Act added a data breach notification requirement to HIPAA, which governs protected health information. The Department of Health and Human Services (HHS) and the Federal Trade Commission (FTC) respectively issued rules for HIPAA covered entities and vendors of personal health records setting forth the parameters for notifying individuals of data breaches involving unsecured protected health information. The HHS and FTC rules both include the following requirements:
  - sending written notice to individuals within 60 days of discovery of breach of unsecured personal health information;
  - sending notice to HHS or the FTC, as applicable; and
  - notifying the media if 500 or more individuals in a state are affected.

The HHS rules expressly include a risk of harm threshold, while the FTC rules do not. Specifically, the HHS rules state that notification to individuals is required only if a breach "poses a significant risk of financial, reputational, or other harm to the individual." The FTC rules require individual notice of the unauthorized acquisition of identifiable health information. The FTC rules presume that when there has been unauthorized access to information (the opportunity to view data), there has been unauthorized acquisition (actual reading or viewing of the data). That presumption is rebuttable, so some risk of harm threshold may be available.

DATA SECURITY REGULATION

Apart from breach notification laws, many other state and federal laws regulate data security. Although a detailed discussion of specific data security regulations is outside the scope of this Note, data security regulations often include requirements for:

- Maintaining reasonable data security of personal information.
- The proper disposal of personal information.
- Additional protection for certain types of highly sensitive personal information, such as Social Security numbers.

REQUIREMENTS FOR REASONABLE SECURITY

Numerous state laws (including California) and federal laws such as GLBA and HIPAA require companies to maintain reasonable data security, and some regimes go into great detail as to what constitutes "reasonable." Regulations that went into effect on March 1, 2010 in Massachusetts (*201 C.M.R. § 17.00*), for example:

- Contain detailed standards for the protection of personal information (as defined in the regulations).
- Require the implementation of a comprehensive, written information security program.

The Massachusetts regulations, which purport to apply to any business holding personal information on Massachusetts residents, even businesses located outside the state, also require, to the extent technically feasible, the encryption of personal information on all laptops and other portable devices, and of personal information transmitted wirelessly or across public networks.

Nevada similarly has an encryption requirement for personal information transmitted across public networks (*Nev. Rev. Stat. § 597.970*).

DISPOSAL OF RECORDS CONTAINING PERSONAL INFORMATION

Certain state and federal laws also dictate that a business's disposal of personal information be done in a secure manner. For example, the FTC enacted rules pursuant to the Fair and Accurate Credit Transactions Act requiring companies that have records containing consumer reports or derived from consumer reports to take reasonable steps to protect the records when disposing of them. The FTC provided examples, including the burning, pulverizing or shredding of paper records and the destruction or erasure of electronic media containing personal information so that they "cannot practically be read or reconstructed." California law typifies the handful of states that have personal information data destruction requirements and it states:

> "A business shall take all reasonable steps to dispose, or arrange for the disposal, of customer records within its custody or control containing personal information when the records are no longer to be retained by the business by (a) shredding, (b) erasing, or (c) otherwise modifying the personal information in those records to make it unreadable or undecipherable through any means" (*Cal. Civ. Code § 1798.81*).

SPECIAL RULES FOR CERTAIN KINDS OF PERSONAL INFORMATION

Numerous states (for example, Connecticut) have enacted laws governing the use, maintenance and disclosure of Social Security numbers, and at least four states specifically require written policies governing the protection of Social Security numbers which in certain circumstances must be available to consumers or employees.

There are also certain federal data security requirements such as regulations enacted pursuant to GLBA for financial institutions and HIPAA for certain health records. As states and the federal government continue to enact and amend data security rules and regulations, compliance with these varying requirements becomes increasingly difficult. Companies operating in the US, or even holding personal information regarding US residents, must monitor requirements and developments to ensure compliance.

AUTHORS

Lynda K. Marshall is a Partner and Timothy P. Tobin is an Associate in Hogan & Hartson LLP's Antitrust, Competition and Consumer Protection practice group. Lynda counsels clients on a variety of data protection matters, including global compliance, privacy audits, internal company policies and data transfer issues. Tim's practice focuses primarily on privacy and data security law matters.

Lynda K. Marshall
Partner
HOGAN & HARTSON LLP

Timothy P. Tobin
Associate
HOGAN & HARTSON LLP