FOR METRO AREA IN-HOUSE COUNSEL

ALM

New York Law Journal

GC New York

Thursday, March 15, 2007

Sharing Business Information In a High-Risk World

BY WILLIAM A. TANENBAUM

THIS is the inaugural column on privacy and data protection. The column is designed to assist general counsel in addressing the privacy and data issues that arise in a "stand-alone" context, such as liability for the wrongful disclosure of consumer personal information, and as part of large corporate initiatives, such as outsourcing, business services partnerships, structuring relationships with information technology (IT) vendors and securing intellectual property protection for databases (copyright) and business methods (patent).

The topics addressed in this column will be based on three fundamental premises. First, today's methods of doing business require a company to open its computer systems and data to third parties. More openness means more security risks. The result is that in-house counsel must work with chief information officers and other business executives to balance the benefits of openness with the increased risks to computer and data security.

Second, privacy is part of a larger category, and I will call that category "information management." This category includes trade secrets, corporate data protection, data exchange, data mining, IT security, protection against competitive intelligence, and information life-cycle management.

Third, data protection should be driven down to the data level. Focusing only on firewall protection is like building a fortress and then failing to take into account all the doors and windows that were inserted in the walls to enable data to flow to and from the castle domain. The data has to move in and out of the fortress, and it needs to be protected as it does, as required by the nature of a specific piece of information and the uses to which it will be put. Broadly speaking, protection in this context means that restrictions need to be in place so that exchange of data does not violate applicable privacy laws and so that confidential and proprietary business data does not lose its proprietary status and enter the public domain.

These three premises, which will be discussed in greater detail below, illustrate the convergence of privacy, security, cybercrime and intellectual property.

All this is reflected in agreements governing customer data, outsourcing and business services transactions, and relationships with information technology vendors. These contracts should be revised to incorporate best practices in privacy and data security protection, and include IP licenses of the proper scope and duration. For example, and as also discussed below, trade secret-style confidentiality agreements may need to be modified to avoid authorizing unintended disclosure of personally identifiable information. In addition, in outsourcing agreements, each party should appoint a data manager as well as a project manager. Furthermore, a company with multiple outsource providers should consider using common contract provisions and service level agreements in order to enable providers to exchange protected data with one another.

Before discussing the three fundamental premises, it will be useful to define "privacy," "corporate data" and "corporate policies" in the security arena. "Privacy" generally means personally identifiable information concerning natural persons, such as name, address, Social Security number and information which is associated with or can be used to identify an individual, such as a credit card or passport number. "Corporate data" is information that relates to a company's business and includes trade secrets and proprietary information as well as operational data that may or may not need to be treated as confidential, depending on the circumstances. It also includes the databases and all the information stored there.

Privacy and corporate data can overlap. For example, when a customer is a natural person, customer data will include personal information that may be subject to a privacy law regime. In addition, when corporate data includes information about employees, it can include health care information which can be subject to the Health Insurance Portability and Accountability Act (HIPAA).

William A. Tanenbaum *is a partner and the chair of the technology, intellectual property and outsourcing group, and heads the privacy practice, at Kaye Scholer LLP.*

There is an obvious IT component to privacy and corporate data protection. The information technology includes the hardware and software used to provide the infrastructure and run the computer servers and databases, the encryption used to transmit data and the biometric authentication technology to establish that an employee is authorized to have access to a database or to a physical location such as a data center.

"Corporate policies" are internal rules adopted by the corporation to govern the privacy and security, and may be more or less restrictive than the law, depending, among other things, upon the jurisdiction and the nature of the corporate transactions. For example, in a global outsourcing to multiple countries using multiple vendors, a company may require all of its outsource providers to adopt a "highest common denominator" data policy in order to minimize legal risk in transmitting data across the borders of countries with different privacy laws.

Each of the three premises outlined above will now be addressed in greater depth.

Openness and Security

As noted, contemporary business practices require a corporation to provide access to its data and computer systems to a range of third parties. These include a company's customers, suppliers and business partners. Sharing information with suppliers is necessary for real-time supply chain management and inventory control, and business partners include domestic and offshore outsourcing providers. A company will often have multiple outsourcing providers located in different countries, and a company's information management practices will need to require—and enable—the vendors to share information with one another in the course of providing services to their common client, namely the company.

Put another way, as a company outsources different business functions to different business process outsource providers, it will need to make parts of a common set of corporate data available to all providers. It will also need to take data that was "processed" by one vendor for one purpose and provide it to another vendor for another purpose. In some cases, the most efficient information flow will require that outsourcing vendors exchange data directly with one another and simultaneously comply with applicable laws. For example, customer data from an offshore call center vendor may be shared with the company's advertising agency and the company's internal marketing division, and at the same time the offshore call center may need to comply with the Federal Trade Commission's "Do Not Call" restrictions when placing outgoing sales calls.

In general, current business trends lead to increased interconnectivity and automated data sharing, and using the Internet as the infrastructure for data sharing highlights the need to balance openness with security and privacy protection. As a result, general counsel will need to work closely with the Chief Information Security Officer and the Chief Privacy Officer in balancing the day-to-day advantages of openness with these increased risks. Today's contracts will control tomorrow's risks, and in-house counsel must look over the horizon to anticipate and address them.

"Contemporary business practices require a corporation to provide access to its data and computer systems to a range of third parties. These include a company's customers, suppliers and business partners."

Information Management

The second item outlined above is the suggestion that "information management" be used as a new paradigm for how lawyers treat privacy and data protection. It provides a systematic approach to handling personally identifiable information (PII), corporate data that includes both PII and non-private but proprietary information, and the movement of data both within a company and between companies and third parties. It also provides a way to integrate privacy and confidentiality requirements with physical and computer security and ways to protect against cybercrime. For example, a third party's access, by hacking or otherwise, into a company database may be a criminal violation and protecting the proprietary information of a company may require the assistance of law enforcement. As a practical matter, in order to get law enforcement agencies involved, it often will be necessary to convince them of the high commercial value of the information which has been stolen, and to present a case that is easy to investigate and prosecute. This is one area where intellectual property protection can provide evidence of commercial value.

Internet search adds a new dimension to information management. For example, for both corporate employees conducting business and individuals acting as consumers, today's important computer tools are Internet browsers and search engines. Many companies are looking at the searches typed into Google search bars to name their products (and get higher rankings in search results) and even to decide what features to include in future products. In other words, they are looking at what people search for as a way to identify commercial demand, and then using the information collected from search requests to design products to meet that demand. It is the search requests—not necessarily the search results—that reveal the products waiting to be created. This is but one example of the commercial value that attaches to information, and how information itself can be an asset worth protecting through the various avenues provided by IP law.

Information management recognizes that the data needs to be categorized in a sophisticated manner. For example, some data will constitute PII, some will be protected by IP, some will belong to a third party and be subject to license restrictions, and some will be public domain data. For information management purposes, information should be assigned to different legal categories, using multiple axes of analysis, and the company should then apply the applicable laws and corporate policies to the applicable categories. Some data will be in multiple categories, thus will be subject to different sets of laws and corporate policies depending upon the nature of different uses of the data,

the laws of the countries involved and even whether it is used within the company or shared with external parties.

This also illustrates the third premise discussed at the beginning of the article, namely, the need to drive data protection down to the data level. In other words, it is not sufficient to protect a company's computer network against intrusions and hackers. It is also necessary to apply privacy restrictions and data protection to individual pieces of information and different categories of data in order to comply with applicable laws governing PII, trade secrets, intellectual property, and to implement compliance with a company's data use and data security policies both within a company and by its third-party partners.

This is often done at the contract level, as shown by the issues raised by confidentiality agreements. Confidentiality agreements are often used to impose nondisclosure obligations on the recipient of personally identifiable information. Such agreements can fail to achieve this purpose, however, if they contain the "standard" trade secret-type exception to confidentiality for material which is in the public domain. This is because personally identifiable information may be in the public domain at the same time that it is restricted against disclosure by law or regulation. For example, an individual's address or other PII may be on file in the county clerk's office as part of a real estate filing or other government submission. However, the availability of such information in a document that is subject to public inspection will not generally relieve a company of its obligation to keep confidential PII which it collected pursuant to a privacy policy or which it is obligated to maintain in confidence subject to a government regulatory regime such as HIPAA or Gramm-Leach-Bliley. A solution to this potential problem is to create an exception to the exception. Thus, a "boilerplate" confidentiality agreement should be modified to provide that the recipient must maintain PII in confidence even if it may be in the public domain.

Tips on Contracts

In the outsourcing context, a confidentiality agreement should be entered into at the RFP (request for proposal) stage before the master agreement is signed. Potential vendors may need to receive confidential information in order to prepare their proposals, and confidentiality must be maintained by a vendor even if it does not get the contract. In addition, because a company may be outsourcing to cure a deficiency in its own business practices, a potential vendor's assessment of those practices should be made confidential to avoid public disclosure.

Contracts should be used to implement the data categorization discussed above and to give legal effect to the categorization by requiring business partners to comply with the company's policies and applicable law. When a company retains more than one outsource provider, there are advantages to having common contract provisions and service levels. For example, the company should create a document that can be used as a schedule in these agreements that sets out the corporate data privacy and IT security policies to which all vendors must adhere. Furthermore, the company's IT security department should conduct a "gap" analysis to determine the areas in which a particular vendor's security practices do not meet the company's standards, and a schedule specifying what steps must be taken to close the "gap" should be made part of the contract.

Certain software and other technology will be sufficient, or in some cases, necessary, to meet the company's security requirements, and when this is the case, the schedule should specify the technology to be used. The schedule should also provide implementation and acceptance milestones so that the "gaps" are closed on a timely basis and penalties imposed if they are not.

An outsourcing agreement can also provide that the data will be given by the provider in either a technology-neutral format or in a particular format that is required by the company's computer systems. The format requirement should also be used to ensure that all of the company's outsourcing providers can readily share and exchange data. Encryption is often required for data security, but not all data encryption is equal. When data encryption is required, both the level of encryption (which defines how difficult it is to defeat the encryption) and the specific commercial encryption product to be used should be specified so that data can be easily used by all parties and so that there is no "weak link" in an otherwise strong chain of transmission. In the outsourcing context, outsource providers should be required to cooperate with a company's other providers, and this often requires modifying provisions in standard vendor form agreements.

Outsourcing and business services agreements should be drafted to provide an "early warning system" to the customer of potential privacy and data security problems. This can be accomplished by requiring vendors to provide reports at specified intervals (tied to the severity of a potential problem) or when certain events occur, such as unauthorized access by third parties. In addition, security obligations should be subject to both electronic and physical audits backed up by penalties to provide a company with the opportunity and leverage to identify and require corrections to technology failures and deficient security practices.

Finally, the benchmarking provisions of the agreement should require that privacy and security benchmarking is not limited to the firms in a company's specific industry. Instead, the benchmarking should be done against the companies that are the "best of breed" in the field even if they are in another industry.

In conclusion, privacy, data security and information management provide both a particular set of challenges and a set of opportunities to commercialize the value of a company's information. Knowledgeable general counsel can avoid the problems and maximize the opportunities, combining best practices with sophisticated contract provisions backed up by practical means to monitor compliance with privacy and security requirements.