Ten Data Security Questions Faced by Every Company

PAUL BOND

Ten commonly asked company security questions are considered in this article.

Personal data collected by companies is at risk from all sides. Thieves want to steal and resell personal data. Employees are tempted to misuse personal data, sometimes for monetary gain, sometimes to satisfy idle curiosity.

Even standard business processes pose risks to personal data. Businesses collect, store, use, share, and dispose of personal data every day. Each of these inflection points is an opportunity for something to go wrong, for a law to be broken or a data subject put at risk.

For data security issues, putting out fires once they are already burning is no longer enough. Increasingly, the law requires a preventative approach. No system is perfect, and there can never be any absolute guarantees against the loss, theft, or misuse of personal information. However, a comprehensive, rational, and cost-efficient legal approach to data security will answer all of the following questions.

Paul Bond is an associate and member of the Global Regulatory Enforcement group at Reed Smith LLP, practicing in the areas of data privacy, security, and management. Resident in the firm's Princeton N.J. office, he may be contacted at pbond@reedsmith.com.

Published in the September 2009 issue of Privacy & Data Security Law Journal.

1. DO YOU KNOW WHICH LAWS AND AGREEMENTS SET FORTH YOUR OBLIGATIONS WITH RESPECT TO PERSONAL DATA?

International, national, state, and private law impose a *de facto* design code on business processes which involve personal information. Business processes must meet code or face potentially severe penalty. Without an ongoing, multisource survey of your data security obligations, it is impossible to even know what goals to adopt.

Create a matrix of your data security and privacy obligations. This may seem overwhelming at first. And, indeed, this is a sizeable, multidimensional task. But start with concrete facts that are already at your fingertips. For example, the applicable data law is often determined by geography.

What Are Your Obligations With Respect To Personal Data *As Triggered By Geography*?

If you are headquartered in, physically present in, employing workers in, selling to consumers in, or even marketing in a certain jurisdiction, you must know the data security and privacy laws of that jurisdiction. The same reasoning applies if you intend to store personal information in a jurisdiction, regardless of whether the information is to be stored in hard or electronic copy.

It is true that local businesses with small geographic footprints may only need to know a few data security and privacy laws. Especially with the maturity of Internet retailing and advertisement, though, many companies which consider themselves local accumulate personal information on a national and international basis, subject to national and international data law requirements.

What Are Your Obligations With Respect To Personal Data *As Triggered By Your Activities*?

Not all triggers for data security and privacy laws are geographic. Industry participation can also trigger application of these laws. For example, banks are subject to financial privacy laws, hospitals are subject

Published in the September 2009 issue of Privacy & Data Security Law Journal.

to medical privacy laws, and Internet service providers are subject to telecommunication privacy laws. But those are easy examples which everyone understands. The real danger occurs when a statute casts a net so broad that it snares companies unaware of their legal obligations. A bank has financial privacy obligations, but so might a used car dealership or a utility company. A hospital has medical privacy obligations, but so might a medical devices company, or any employer. Moreover, the regimes often overlap. A doctor's office that accepts payment by credit card, for example, may have statutory financial privacy obligations, statutory medical privacy obligations, and privacy obligations by dint of its merchant agreement with the issuing cards.

What Are Your Obligations With Respect To Personal Data *As Triggered By Your Agreements*?

In fact, a great number of data privacy and security obligations are not "on the books" at all. These obligations exist by virtue of private agreements. The payment card industry's complex web of obligations, audits, indemnities, and penalties is just the most prominent private regime for the protection of personal information. Especially now that breaches become instant news items, and class action lawsuits follow close after, many vendor agreements contain covenants promising the protection of personal data. These covenants are often material contract terms. Softer than contractual covenants are the occasional notices one company will send another regarding "privacy expectations." These "expectations" letters may not have the force of law, but they are ignored at the recipient's peril. Again, it simply makes sense to catalogue all such covenants and letters as part of an overall matrix of obligations.

2. DO YOU HAVE A COMPREHENSIVE WRITTEN INFORMATION SECURITY PROGRAM?

A company never wants a court or regulator to use the following words in describing its written information security program: haphazard, fragmentary, a patchwork, partial, out-of-date, or worst of all, nonexis-

tent. At the same time, it is often impractical for companies to cabin their information privacy, security, and management efforts in one document. A suite of written policies and procedures is often required. One document may serve as the capstone, stating the aspirations of the company with respect to personal information. Many documents will expand that capstone, describing in greater and greater operational detail how exactly personal information is protected. These documents should be developed with the participation of legal, compliance, and every line of business that the policies and procedures will cover.

Employees will consult these documents when faced with daily "nuts-and-bolts" questions about how to handle personal information. If well drafted, employees will know which documents to consult for which situation, and can either find a concrete answer in the document or be pointed to the relevant decisionmaker, who can provide guidance.

3. DO YOU HAVE A WRITTEN PLAN TO RESPOND TO THE LOSS OR THEFT OF PERSONAL DATA?

Data security breaches, by definition, are emergencies. A company that does not have a coordinated plan for data security breaches will not have time to write one when the siren sounds. Coordination takes time and sustained effort.

The United States is now several years into the era of mandatory data security breach notification. Almost all large companies, and many smaller ones, have already had to give notice of a breach on multiple occasions. Companies must resist the temptation to fall into complacency over their notice preparedness. All but a handful of states have passed notice laws, and each state's law differs from the others in small but important ways. Frequently, states amend their laws to protect more information and/or to require more notice, either notice to consumers or notice to government officials. States want better, wider, faster notice. Add (a) new federal obligations to disclose the loss or theft of protected health information, (b) business-to-business notice covenants, and (c) an increasing demand for transparency in jurisdictions outside the United States. A company must not rely on an old notice plan or old surveys of notice law.

4. ARE YOUR SYSTEMS DESIGNED TO DETECT IDENTITY THEFT RED FLAGS?

In recent years, hundreds of class actions have arisen from the alleged theft of personal data. Data security class action litigation usually focuses not on the (often judgment-proof) criminal wrongdoers themselves, but on the companies those wrongdoers happened to work for, with, or through.

Moreover, governments around the world have drafted businesses into the war against identity theft. Hefty fines can result from a lack of due diligence.

In hindsight, it is always easy to claim that the criminal's activities should have stuck out like a sore thumb. Precautions to detect likely criminal activity, to the extent practicable, are essential for any business's self-preservation.

5. DO YOU HAVE A PLAN IN PLACE SO THAT WHEN MAJOR LITIGATION IS FILED, THE RELEVANT DOCUMENTS, PHYSICAL AND ELECTRONIC, WILL BE PRESERVED COMPANY-WIDE?

Few rhetorical flourishes are more effective than a trial lawyer pointing to the document that does not exist because the defendant destroyed it. Knowing the lifecycle of personal data in your company is only a subset of a broader knowledge of business process. That knowledge lies at the heart of every unified plan of data management.

6. DO YOU HAVE A ROUTINE FOR THE SAFE DISPOSAL OF PERSONAL DATA NO LONGER NEEDED?

Companies need to retain information for business, compliance, and legal purposes. When there is no remaining purpose to keep information, it should be destroyed — safely. The only information that cannot be compromised is information which has been timely and safely disposed of. Improper disposal of personal information is a public relations disaster

Published in the September 2009 issue of Privacy & Data Security Law Journal.

waiting to happen. Picture a reporter standing in a dumpster behind your business, taping a segment about all the personal information he found in your trash. Imagine the reporter and cameraperson have asked an investigator from the Federal Trade Commission along for the ride. Safe disposal of personal information is key.

7. DO YOU KNOW AND COMPLY WITH ALL LEGAL REQUIREMENTS IN THE INTERNATIONAL TRANSFER OF PERSONAL DATA?

Today, businesses operate globally, with technology that knows no national boundaries. Nothing comes more naturally than hitting the "Send" button and zipping information halfway around the world.

But every jurisdiction in the world can claim the right to protect its citizens — and information about them. The United States has a very different conception of "personal information" and adequate protection of it than does the Europe Union; the EU view does not necessarily speak for all of its member states; and some of those states have their own local standards. And so it goes, in every part of the world.

Transfer of information between jurisdictions, by its nature, implicates multiple privacy protection regimes. Many of those privacy protection regimes consider other areas of the world "unsafe." Before hitting the "Send" button, you need to know exactly what data protection protocols are put in place by the relevant jurisdictions.

8. DO YOU MAKE SURE THAT YOUR EMPLOYEES AND VENDORS UNDERSTAND AND FOLLOW YOUR DATA PROTECTION RULES?

A written policy is necessary, but not sufficient to ensure compliance. A written policy without implementation and adherence is a dead letter. Plain language review, easy-to-follow training materials, employee testing, vendor auditing, security breach drills, and the like are indispensible to making sure policy is part of day-to-day procedure.

9. DO YOU REVIEW STATEMENTS TO CONSUMERS (WEBSITES AND ADS) AND INVESTORS (PROSPECTUSES) TO ENSURE THE COMPANY DOES NOT OVER PROMISE ON DATA PROTECTION?

What you promise as to data protection will be held against you. If you fail to meet your promises, legal action and/or government investigations are likely to result. Unless your marketing department and investor relations team are part of your data protection team, they may be working against you by promising too much. Create reasonable expectations and manage them.

10. ARE YOU PROPERLY INSURED AGAINST DATA LOSS OR THEFT?

The last risk you need to plan for is the risk that all other mitigation will, ultimately, not be sufficient. As noted above, no system is perfect. Data privacy and security lawsuits can cost millions or tens of millions of dollars to resolve. The right level of coverage, either under general policies or specific endorsements, is something that every company needs to determine on an ongoing basis.

Companies will never be done putting out data security fires. But with effective planning, true emergencies will be less frequent, and easier to put right.

Published in the September 2009 issue of Privacy & Data Security Law Journal.