TITANIC PRIVACY MISTAKES

ICEBERGS LOOMING FOR MULTINATIONAL COMPANIES

BY RUTH HILL BRO

If your client is the largest in the world, uses some of the most advanced technology available, surpasses rivals across the board, has experienced personnel, generally complies with known legal requirements, and has product launches that create a media frenzy, it would be tempting to conclude that your client has little to worry about. Yet that conclusion would be wrong, as all those attributes were used to describe the "unsinkable" *Titanic*, which sunk on its maiden voyage in April 1912.

No one is unsinkable when it comes to privacy/data protection compliance, particularly when it concerns personal data that travels from the EU to the United States (much as the *Titanic* traveled from Southampton, England, on its way to New York City). Rapidly evolving technology and legal requirements pose privacy challenges for even the most experienced companies and particularly those that must navigate uncharted waters throughout the world.

Every company, large or small, will face data protection issues because every company has personal data (regarding customers, employees, etc.) that is regulated in some way in virtually all of the major commercial centers of the world. Many of these countries can impose significant penalties, including criminal sanctions in some cases, for violations.

How can companies avoid *Titanic* mistakes when it comes to privacy? Consider the following cautionary tales.

Privacy: Always a Sea Change

Change is constant when it comes to privacy, and one reason is technology. The Internet, powerful telecommunications networks, and sophisticated digital technologies have created new opportunities for businesses to collect, track, analyze, reproduce, and disseminate personal data, such as names, addresses, phone numbers, email addresses, and a host of other types of information that can be used to identify an individual. Such personal data underpins the business of every company and cuts across every department on an organizational chart:

- It is collected through email, text messages, websites, and extranets.
- It comes by mail, personal courier, phone intake, and face-to-face interaction.
- It is one of the drivers for promotions, sweepstakes, contests, and other marketing efforts.
- Customer and supplier transactions, where credit card numbers and other financial information are collected, depend upon it.
- Companies ask for it whenever they offer a newsletter or encourage individuals to request information.
- It is collected from employees and prospective employees, both offline and online.
- It comes from, and goes to, affiliates, trading/business partners, outsourcing providers, contractors that support the company's business, and other third parties.
- Companies may also collect it from any number of public sources, social networking sites, and purchased databases.

Where data was once stored in the local country in which it was first collected, it is now stored in either regional or, increasingly, global databases, often located in the United States (where a multinational company may have its headquarters) or countries such as India, where the cost of business is lower, and 24/7 service can be provided. But when data is transferred (which includes being accessed from disparate locations throughout the world), a number of data protection issues can arise, including obligations to provide data security, notify or secure permission from data subjects or data protection authorities, consult or secure approval from works councils, enter into appropriate contracts with third parties, and take a legally recognized approach when transferring data outside of the country where the data was first collected.

Companies must likewise contend with privacy issues raised by continuously emerging technological capabilities, including those related to social networking, printer codes, iris scanning, GPS, RFID, search engines, behavioral advertising, and the like. Existing laws do not always lend themselves well to the issues raised by advanced technological capabilities that few could have contemplated when the laws were drafted. Companies should consider to what extent current laws restrict how they use these technologies; even where the company is not restricted by current law in using the technology, the company should evaluate whether its planned usage could result in the company being tried in the court of public opinion (e.g., via adverse media coverage, widespread employee objections, or poor employee morale).

Given the speed with which technology advances, companies should reevaluate their policies frequently, and certainly each time a new technology is deployed in the workplace, on a corporate website, or elsewhere. Otherwise, companies could unwittingly find themselves violating their own policies (which, when applied to new forms of electronic communications, could have unintended consequences), failing to address risks of new technologies, being out of step with emerging legal requirements, or subjecting themselves to adverse media coverage.

Ruth Hill Bro is the immediate past Chair of the Section of Science & Technology Law. She can be reached at ruth.bro@comcast.net.

Still Waters Run Deep: Misperceptions Regarding the EU Data Protection Directive

Many view the EU as setting the highest bar globally when it comes to data protection. Through its Data Protection Directive (Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995), the EU takes a comprehensive approach to data protection that applies to all businesses and all types of personal data and requires companies to provide individuals with notice about information practices, obtain their consent in some cases, only collect personal data that is required to fulfill a legitimate purpose, process personal data fairly and lawfully, give data subjects opportunities to access and correct/delete their own personal data, take special measures with respect to "sensitive" or otherwise special personal data, provide appropriate security for personal data, and so on. Likewise, transfers of personal data to the United States and other countries that do not meet the EU's high standard of data privacy protection (known as the "adequacy requirement") are not permitted without an exception or legally recognized approach (e.g., Safe Harbor, binding corporate rules, or model contracts).

What many do not realize, however, is that the Directive is simply a "minimum floor" for data protection that must be implemented by all member states. Countries are free to fill in the details and impose stricter controls, and many do (e.g., Austria, Belgium, France, Germany, Italy, Poland, Spain, and others). More demanding jurisdictions may require approvals from data protection authorities (for both collection/processing and cross-border transfers), stricter substantive requirements (e.g., notices must contain "exhaustive" and not merely "illustrative" lists of the purposes for processing), greater limits on the use of cookies in the Internet environment, and other restrictions. Countries with more requirements may also be more vigorous in their enforcement activity.

These differences mean that companies will need to consider the laws in all relevant EU member states when preparing privacy notices to data subjects, using cross-border transfer vehicles to meet the adequacy requirement and draft corresponding documentation, and the like. Drilling down to this level of detail can be a challenge, especially when budgets are tight. Prioritization is key: the company must figure out what to do first to most cost-effectively meet its objectives, based on a wide range of factors, including the countries where the company has more significant operations, the countries that have particularly strict or specific legal requirements or have particularly active data protection authorities enforcing the law (with correspondingly serious consequences for violations), and the company's assessment of what would be its privacy/data protection nightmare scenarios.

"*Safe* Harbor" Will Not Shelter Companies From All EU Privacy Storms

The EU's adequacy requirement has received considerable attention because it can threaten the flow of personal data that is essential to the business operations of U.S.-based multinationals and companies in other non-EU jurisdictions. Yet many forget that the Directive is broader than just cross-border data transfers**,** which are the focus of the Safe Harbor framework developed by the U.S. Department of Commerce in consultation with the European Commission.

Although Safe Harbor self-certification makes it lawful to transfer personal data to the United States, it does not substitute for complying with the national provisions implementing the Directive that apply to the *processing* of personal data in the various member states. U.S. companies that are "established" in EU jurisdictions will likely need to both comply with applicable

local law in the EU (discussed above) *and* join Safe Harbor (or take another legally recognized approach). All too often, initiatives to legitimize cross-border transfers must be expanded to include long-overdue local compliance.

It is also important to recognize that Safe Harbor is only available to *U.S.* entities. Companies in other non-EU countries lacking an adequacy finding will need to find other ways to legally transfer personal data from EU jurisdictions. Although companies may decide to route everything first through the United States, some don't realize that onward transfers from the United States to other countries can raise special issues that require contractual solutions and careful planning.

At the same time, many companies are surprised to discover that Safe Harbor self-certification (and certain other cross-border solutions) may require notification to or approval from data protection authorities in some jurisdictions and that lead times can vary greatly. Some companies find out the hard way that such filings may reveal that the company has not met the requisite local compliance obligations; thus, it is critical to address these local compliance issues before such filings are made.

Carry Enough Lifeboats: Data Security Breaches Are Not Just a U.S. Issue

Today, virtually all corporate information is created, used, communicated, and stored using digital technology. Although this has allowed companies to reduce expense and increase productivity, it also has made them quite vulnerable to both internal and external threats. Every day, a new corporate data security breach involving the loss or disclosure of personal data is reported in the media. Thanks to laws in nearly all U.S. states requiring that affected individuals be notified of such breaches, the press eventually tolls the bell for all to hear. With each revelation, calls have increased for government investigations and new legislation.

The U.S. Federal Trade Commission (FTC) has indicated that every company must maintain an effective information security program if it is to avoid unfair and deceptive trade practice claims. The FTC's case settlements to date should serve as a navigational chart for all companies when it comes to data security, in that they require companies to: designate employees responsible for information security; identify internal and external risks to the security, confidentiality, and integrity of information; implement reasonable safeguards to address these risks; and test, monitor, and adjust the security program on an ongoing basis. At the same time, state legislation is continually emerging that expressly identifies such obligations.

Data security breaches and the resulting legislative and regulatory responses are increasingly capturing the attention of other government authorities throughout the world. As a result, many countries are starting to adopt, or consider, breach notification laws similar to those in the United States. Even absent country-specific data security breach notification laws or government guidance, notification obligations could still be triggered, such as: (a) from contractual commitments, (b) due to registration of a database with a data protection authority, (c) from obligations in local laws to take reasonable steps to protect personal data, (d) from obligations in local laws to notify the data subjects regarding third parties with whom the data is shared and how the information will be used, and (e) where potential harm could be mitigated by notification.

Ultimately, it is critical for companies to "carry enough lifeboats" by: (a) examining their privacy and security policies and procedures in light of recent events, while keeping an eye out for new laws, with new compliance obligations, that could be on their way; (b) identifying in advance what incidents will trigger compliance obligations under these emerging statutes and what must be done to comply with such laws once a breach occurs; and (c) take ongoing steps to address problem areas.

COMPANIES WOULD DO WELL TO AVOID THE MISTAKE MADE BY THE *TITANIC*'S RADIO OPERATORS, WHO IGNORED WARNINGS FROM OTHER SHIPS ABOUT ICEBERGS IN THE AREA.

Off the Radar Screen: The Dangers of Workplace Monitoring Outside the United States

The dangers of workplace monitoring outside the United States are off the radar screen of many companies, some of which have had officials criminally sanctioned for violations of local law. Companies would do well to avoid the mistake made by the *Titanic*'s radio operators, who ignored warnings from other ships about icebergs in the area.

About two-thirds of U.S. businesses electronically monitor employees in some fashion, given concerns about data security, workplace harassment, and lost productivity, but the ground rules for such monitoring are far from clear. At the same time, as technology increasingly blurs the line between work and home and also facilitates more sophisticated monitoring, concerns about privacy are escalating.

Although there is no omnibus federal law in the United States that explicitly addresses workplace monitoring of electronic communications, a number of federal laws preclude workplace monitoring in certain circumstances, and some states have added statutory requirements (e.g., Connecticut and Delaware impose a notice obligation).

Nevertheless, U.S. employers have considerable flexibility in monitoring their employees. At the same time, however, many EU member states have become increasingly aggressive in regulating electronic monitoring in the workplace, leaving U.S. employers wondering how to deal with such issues both domestically and globally.

Establishing (or updating) the company's electronic communications policy plays a vital role in addressing such issues. The need is particularly keen for multinational companies, including those that have gone global with respect to HR data and centralized IT staffing. Yet, the sort of electronic communications policy that an employer should have in the employer-friendly United States should not be rolled out globally, especially in EU countries, where privacy may be viewed as a fundamental human right. "Icebergs" in U.S. electronic communications policies that could cause problems for multinational companies include:

- *Treatment of personal email.* Blanket prohibitions against personal email or reservation of the right to review personal email may run afoul of many countries' laws, especially in the EU.
- *Broad purposes for monitoring.* In countries with privacy laws, the employers' purposes for monitoring will be limited to legitimate business reasons. Some jurisdictions require a list of the exclusive purposes of the monitoring and the categories (and the location) of recipients of the information collected.
- *Indefinite storage of the collected data.* Some countries impose limits on how long information can be stored; some require that the employer disclose both the retention period and the storage locations.
- *Failure to specify access, correction, and other rights.* In some jurisdictions, the rights of the employees must be expressly spelled out in the policy.
- *Not mentioning that personal data may be transferred* to the United States or otherwise outside of the employee's jurisdiction. Companies often do not realize that when the server is elsewhere, or when the U.S.-based IT staff accesses non-U.S. employee communications, that a cross-border transfer of the data occurs. Many countries require notice to employees that such transfers will occur (the particular country receiving the data may need to be specified), as well as identification of the legal basis for making the transfer.
- *Requiring employees to report violations* of internal policies by other employees. The ability to impose such obligations is restricted in some jurisdictions, especially in the EU.
- *Engaging in systematic and widespread monitoring.* Monitoring of employee communications can be a controversial and unsettled issue, and the ability to do so may be extremely limited in some countries, with criminal penalties for not getting it right. Any monitoring needs to be performed in accordance with local law and be proportionate to the risks at issue.

SOS: Other International Privacy Issues That Pose Dangers

Companies must navigate around these and other icebergs when it comes to privacy in international waters. Other privacy issues that could sink a company include:

- *emarketing* (not recognizing that the United States opt-out approach won't work in the EU),
- *anonymous Sarbanes-Oxley whistleblower hotlines* (which can run afoul of other countries/data protection and labor laws if not carefully structured), and
- *ediscovery* (where powerful software that automatically searches workers' computers and sends it back to the U.S. parent for investigation and production can violate data protection laws).

More often than not, however, the biggest iceberg that could sink a company is of its own making. Some companies underestimate the time, effort, and resources it will take to develop privacy policies and procedures that comply with applicable law and reflect actual information practices, to the extent such practices are even known or understood. The complexity is particularly great when working across multiple jurisdictions. Rushing to launch a "form" privacy policy that does not truly reflect the company's information practices can result in the company saying one thing and doing another. Government enforcers, in the United States or elsewhere, will not hesitate to hold a company to the promises it makes in policies and other areas, including in its own code of conduct/ethics, where one often sees promises to comply with the letter and spirit of the laws in every jurisdiction in which the company operates.

Charting a Safe Course

Penalties for noncompliance with foreign privacy and security laws can be far more severe than in the United States. In most jurisdictions, the penalties can include injunctive relief that restricts a company's ability to collect, use, transfer, or otherwise process personal data, which can have a profound impact on a company's operations. The potential penalties can include substantial fines, with some of the highest being in Spain (which has a particularly active data protection authority), where fines of $600,000 per violation could be imposed. Potential prison terms for corporate officers for serious violations are far more prevalent outside the United States, with some of the highest being in France, where prison terms can reach five years. Although many companies are willing to pay fines for privacy noncompliance, few have employees willing to go to jail for such noncompliance.

Despite increasing warnings of icebergs ahead that can sink even the greatest of enterprises, there are those that will move full speed ahead, plunging into the darkness, oblivious to the dangers. Prudent companies are now taking steps to avoid the *Titanic* privacy mistakes that can cause even the biggest and the best to founder. ◆