Westlaw Journal
AVIATION

Litigation News and Analysis • Legislation • Regulation • Expert Commentary

VOLUME 29, ISSUE 23 / JANUARY 9, 2012

Expert Analysis

Top 5 Commercial Data Security And Privacy Issues in 2012

By Cynthia J. Larose, Esq.
Mintz Levin

As numerous industry and regulatory trends continue to converge, 2012 promises to be a watershed year for online commercial data security and privacy. Companies could be forced to change how they store and use customers' personal information. At the least, businesses must ensure they have robust processes and systems in place to protect private data.

Here are the top five issues to keep a close eye on in 2012.

CYBER SECURITY

Cyber security will be a central concern for businesses in every industry. Exhibit A of the need for redoubled vigilance is the continuing fallout from the massive data breach of Sony's online video game network.

Last April Sony suffered one of the largest ever Internet security break-ins when hackers stole millions of customers' personal information, including birth dates, email addresses, user names, passwords, logins and security questions. The security breach could ultimately cost the entertainment giant over $1 billion.[1]

In its rush to deliver new online products, Sony likely did not pay enough attention to security when developing software to run its network. While Sony's security meltdown was a headliner, other well-known companies were also hit by major hack attacks, including Chase, Citigroup, Best Buy and Walgreens. Citigroup, for example, during a routine monitoring of its commercial data, discovered the theft of names, account numbers and email addresses of over 200,000 customers.

The ramifications of a security breach include the cost of rectifying the breach, performing security investigations, customer notification, network repairs, marketing costs and substantial lost revenues.

Data breaches can also expose a company to a variety of lawsuits. Sony faces a class action alleging it failed to encrypt the stolen data, establish adequate firewalls and provide prompt, adequate warnings of security breaches. In addition to a class action, other potential security breach claims are shareholder lawsuits, as well as

Policymakers are primarily concerned with consumers' lack of understanding of the ubiquitous collection and use of their private information and their lack of ability to make informed choices about it.

suits by credit card issuers for the cost of reissuing credit cards and investigating credit card fraud.

To minimize these business and legal risks, companies should always conduct periodic risk assessments and update their data control mechanisms. It is essential to embed data privacy into software designs to make customer privacy the "default setting."

Protecting customer privacy proactively should be entrenched in everyday business practices, along the lines of:

- Assessing what information needs to be secured and where it is located
- Restricting administrator access to that information and scrambling the data to make it unreadable
- Having ample documentation of security systems in case government regulators decide to investigate.

LEGISLATIVE AND REGULATORY ACTIONS

Online data privacy has captured the attention of policymakers in Washington and at the state level.[2] The result could force companies to:

- Devise more robust data security plans.
- Regulate how they collect, maintain, secure and use private data.
- Develop more transparent policies for the data they collect and share with third parties.

A dozen bills have been filed in Congress. A leading measure in the Senate would force companies to bolster data security practices and notify consumers whose information is stolen. The fate of the bill is uncertain, as lawmakers are divided over what information should be covered, the role of the Federal Trade Commission in enforcing a new law and the relationship of the federal law with existing state laws on data breach notification.

A prime example of the heightened regulation of online privacy is the recent settlement between Facebook and the FTC regarding how the social network adjusted privacy settings without user consent. The settlement will, among other things, require Facebook to implement a comprehensive written privacy program for its products and services. The settlement also subjects Facebook to 20 years of independent privacy audits certifying its compliance with all of the provisions of the FTC consent decree. In announcing the settlement with Facebook, FTC Chairman Jon Leibowitz said "Facebook is obligated to keep the promises about privacy that it makes to its hundreds of millions of users."[3]

Policymakers are primarily concerned with consumers' lack of understanding of the ubiquitous collection and use of their private information and their lack of ability to make informed choices about it.[4] Another trend troubling regulators is the blurring distinction between personally identifiable information and supposedly anonymous or "de-identified" information.[5] At the same time, however, they want to continue encouraging e-commerce innovations.[6]

This balancing act will continue to define the debate.

Also on tap is the expected release of the final reports on online privacy from the FTC and the U.S. Department of Commerce. A year ago, both agencies released lengthy reports on consumer privacy protections and received extensive comments from stakeholders, but they have not yet completed their final reports.

The FTC's report included a "Do Not Track" recommendation for an opt-out path for consumers who do not want their online browsing activities made available to third parties.[7] The agency did not call for mandatory regulations, but rather voluntary compliance and cooperation among browsers, computer makers and advertisers.

To be effective, Do Not Track requires a persistent setting (such as a cookie) on consumers' browsers signaling their choices about being tracked and receiving targeted ads. Leibowitz most recently told a digital advertising conference that the commission is "heartened" by industry efforts at voluntary compliance and enforcement, but it is "not yet universal," and the issue is still alive in Congress.[8]

NAVIGATING U.S. PRIVACY REGIME AND THE REST OF THE WORLD

More countries are adopting privacy laws in line with the European Union model, which focuses on the privacy interests of the individual. India in 2011 adopted new privacy regulations similar to prevailing EU privacy laws.

The EU approach to protecting privacy — comprehensive national laws, prohibitions against collection of data without a consumer's consent and requiring companies that process data to register their activities with government authorities — is in stark contrast to the U.S. approach, which to date has been more ad hoc and industry-based. The U.S. privacy model is a mixture of laws, regulations and industry self-regulation rather than a single, comprehensive federal data protection law. Free market and freedom-of-speech principles predominate.

The fundamental idea of the EU's 1995 Data Protection Directive[9] is that personal data should not be processed except in limited circumstances. Each EU nation has since passed its own national privacy law similar to the directive. These laws apply when a company is doing business or using equipment in the EU.

As privacy laws are internationally trending toward the EU model, U.S. businesses need to assess the way they do e-commerce abroad because compliance with foreign data protection rules and regulations may require them to change their business practices. Conflicting foreign data privacy requirements pose an obstacle to implementing global information management systems and imposes significant costs in tracking and complying with data protection laws in each country.

The 2009 EU Cookie Directive[10] is another major restriction on the collection of consumer data. The Cookie Directive calls for tighter regulations on the way companies track online customers for behavioral advertising and targeted marketing. Users are to be given a greater opportunity to opt out of receiving certain types of cookies on their personal computers.

Last August France passed a law consistent with the directive, requiring consumer consent before certain types of cookies are placed on personal computers. The UK recently passed a similar law requiring businesses and organizations to obtain informed consent from visitors to their websites in order to store information on users' computers.

A key consideration for 2012 is whether the government will continue to rely on industry self-regulation for cloud computing or whether the FTC will issue comprehensive rules.

CLOUD COMPUTING WILL CONTINUE TO RAISE PRIVACY CONCERNS

Cloud computing enhances the ability to collect and centrally store consumer data and to share that data with third parties.

Amazon's recently launched Kindle Fire comes preloaded with a cloud-based Web browser (known as Silk), which allows Amazon to capture and control every Web transaction performed by Fire users and filter that data through its cloud server.

Other companies, such as Google, Microsoft, Amazon and Facebook, offer an array of cloud-hosted applications for customers. Cloud applications are cost-effective and allow companies to access computing resources and storage that would be out of reach for on-premise installations.

Not surprisingly, privacy advocates are ringing the fire alarm over this increased tracking of consumer information. A key consideration for 2012 is whether the government will continue to rely on industry self-regulation for cloud computing or whether the FTC will issue comprehensive rules.

Other emerging cloud computing issues come from abroad. First, European governments are increasingly concerned that U.S. companies will turn over their citizens' private information to the U.S. government if demanded to do so under the Patriot Act. This would contravene European law, which bars organizations from divulging data to a third party outside the European zone without the user's permission. The Netherlands has banned U.S. cloud suppliers from Dutch government IT contracts as a result. This could happen in other European nations.

The other major cloud issue is the location and movement of the data under E.U. data protection laws. Cross-border transfer of personal data to a jurisdiction that is deemed to have "insufficient" protection by the E.U. is only permitted under certain circumstances, usually with the data owner's express consent. Data in the cloud could be collected, processed and stored in many different locations, all very removed from the data owner.

The data protection issues inherent in the cloud computing model are under discussion by the Article 29 Working Party, responsible for data protection issues at the European Community level. This will likely lead to controversy in the year to come.

LOCATION-BASED SERVICES WILL LIKELY GROW AND BE OF GREATER CONCERN

Location-based services pinpoint geographic locations via mobile devices and are increasingly being used in e-commerce. For example, users can tell a social network (*e.g.*, Facebook Places) they are visiting a retail establishment in order to get a coupon for discounts and prizes. LBS can also help find a nearby restaurant or ATM. The uses of LBS are wide and varied.

Location information is often then shared with advertisers who like to know where and when someone has been so they can target-advertise. Not surprisingly, this has raised the hackles of privacy advocates, who claim the access to location history is often done without user consent. According to a Nielsen study of U.S. smartphone users last April, many consumers are reluctant to "check in" via an LBS because of privacy concerns.

In response, some LBS vendors are requiring explicit opt-ins, reduced positioning accuracy and other privacy protections. Though social networks and other LBS

vendors may have robust privacy policies, protection against the leaking of private information to third parties is certainly not ironclad.

Policymakers in Washington and abroad will continue to grapple with the legal framework for regulating the privacy aspect of location-based services. Best practices and self-regulation for mobile phone providers, technology companies and equipment makers will continue to evolve as well.

NOTES

1 *Sony data breach could be most expensive ever*, Christian Science Monitor, May 3, 2011, *availavle at* www.csmonitor.com/business/2011/0503/sony-data-breach-could-be-most-expensive-ever.

2 *See, e.g.,* Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework, U.S. Department of Com-merce, *availavle at* www.ntia.doc.gov/files/ntia/publications/iptf_privacy_greenpaper_12162010.pdf.

3 Press Release, Federal Trade Commission, *available at* http://www.ftc.gov/opa/2011/11/privacysettlement.shtm.

4 FTC, Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers (December 2010), *available at* www.ftc.gov/os/2010/12/101201privacyreport.pdf.

5 *Id.*

6 *Id.*

7 *Id.*

8 *DAA should partner with browsers on Do Not Track, says FTC chairman*, Direct Marketing News, Nov. 8, 2011, *available at* http://www.dmnews.com/daa-should-partner-with-browsers-on-do-not-track-says-ftc-chairman/article/216325/

9 Directive 1995/46/EC.

10 Directive 2009/136/EC.

Cynthia J. Larose is a member of **Mintz Levin**'s corporate and securities section in Boston and chairs the firm's privacy and information management practice. As a certified information privacy professional and represents companies in information, communications and technology, including e-commerce and other electronic trans-actions. She can be reached at cjlarose@mintz.com