Wednesday, December 30, 2015

Privacy and cybersecurity laws becoming ever more complex

By Joshua Sebold

Joshua Sebold / Daily Journal

Paul M. Schwartz, a special adviser for Paul Hastings LLP

Privacy and cybersecurity law continued to grow in importance, influence and complexity in 2015, and attorneys specializing in these fast-developing practice areas say it is difficult to imagine that the same won't be true next year and beyond.

Technology companies in Silicon Valley and throughout California saw significant regulatory changes at the state, national and international levels, but the European Court of Justice dwarfed all other developments in the field when it invalidated the Safe Harbor agreement that allowed companies to efficiently transfer data between the U.S. and Europe.

On the national level, the Federal Trade Commission cemented its role as a regulator of data breaches, and on the state level, tech companies applauded the passage of an update to California's version of the Electronic Communications Privacy Act that makes it more difficult for local law enforcement to access data without a search warrant.

Many privacy attorneys representing international tech companies thought Russian President Vladimir Putin was the biggest thorn in their side - until the final quarter of the year.

Putin instituted a rule decreeing that all data originating in Russia should be stored and primarily processed on Russian soil, which left companies scrambling to build data centers or create joint ventures with existing data center owners in the country. Putin's move was considered extreme at the time, but soon the EU proved that the concept of restrictive "data sovereignty" was more universal.

"Every single month I was calling my Russian lawyer and saying, 'What are they doing, what does it mean?" said Francoise Gilbert, a Greenberg Traurig LLP shareholder. "Now the only thing I talk about is Safe Harbor."

There are more options to transfer data between most European countries and the U.S. than there are to move data out of Russia, but the sheer scope and variety of European regulatory regimes has created a much larger headache that affects many more companies.

The Safe Harbor agreement, which had been in place since the year 2000, allowed companies to move data across borders through a relatively uniform regulatory system.

Now, companies receiving or transferring data across borders need to sign individual agreements that comply with each individual country's regulatory system.

"I've been told that 1,600 companies have letters from the Spanish data protection commissioner saying they have to submit a plan to come into compliance before January 29," said Maureen S. Dorney, founding partner of Paradigm Counsel LLP.

Dorney said the sudden change in EU law has made life difficult enough for individual companies trying to manage their own operations, but it's caused even more disarray in negotiations involving mergers or business-to-business agreements between companies that handle international data.

Experts say merging with a company that has been secretly hacked can lead to major liability from customers and shareholders. Acquiring a company that isn't in compliance with U.S. or international regulators can also prove expensive.

Dorney said these added risk factors have slowed deals with additional due diligence work or scuttled them completely.

"The uncertainty that exists right now is causing chaos in business negotiations," she said. "The lack of a unified approach is actually costing the economy a lot of money."

At the national level, however, the regulatory picture became a bit clearer this year. The Federal Trade Commission got an endorsement for its cybersecurity and data breach enforcement authority from the 3rd U.S Circuit Court of Appeals in its case against Wyndham Worldwide Corp., a hotel chain that suffered repeated data breaches.

Wyndham suffered three major cybersecurity breaches in a span of two years, losing data belonging to hundreds of thousands of its customers. The court ruled that the FTC does indeed have authority to regulate consumer privacy and remanded the case to district court.

Although its scope is more limited, the Federal Communications Commission has also made moves to establish itself as a privacy regulator. Paul M. Schwartz, a special adviser for Paul Hastings LLP and co-director of UC Berkeley's Center for Law & Technology, said the FCC actually established itself as a more aggressive regulator than the FTC, despite its shorter track record addressing privacy issues.

"The FCC has already announced greater fines over the last two years than the FTC has done in however many years," he said.

Schwartz pointed to a $25 million settlement AT&T Inc. agreed to in April. The FCC announced the settlement as the largest data security enforcement action in U.S. history.

Meanwhile, California moved a little closer to Europe in terms of the balance between law enforcement and personal privacy with its revamp of the state's Electronic Communications Privacy Act, which prevents local and state law enforcement from collecting data without a warrant under most circumstances.

This will make it almost impossible for law enforcement to use "stingray" devices to monitor cell phones and track their owners' locations unless they're working with a federal law enforcement agency.

The rule change also prevents law enforcement from searching cell phones during traffic stops and mandates that investigators get a warrant before forcing tech companies to hand over user data.

Tanya Forsheit, a partner at Baker & Hostetler LLP, said the move was widely applauded by privacy analysts with European sensibilities. She said that many tech companies would prefer if California was its own country, because the state's stances on protecting personal privacy are becoming increasingly closer to Europe's. She said much of the tension between European regulators and the U.S. stems from persistent distrust of the National Security Agency.

"If the U.S. was operating in the same way California was, I don't think we would

have the degree of problems we have with Europe so far," she said.

joshua_sebold@dailyjournal.com