Privacy regulations increasingly unwieldy heading into 2017

By Joshua Sebold

The Daily Journal, December 29, 2016
http://bit.ly/2iKuU0X

The rash of online privacy laws and regulations continued to grow in size and complexity last year, and there is little reason to believe 2017 will be any different.

Times are busy for privacy attorneys, but they are not predictable.

The dizzying array of expanding regulations from various federal agencies, foreign countries and state governments is almost an unmanageable amount of information for business leaders and their advisers to track, said Paul Hastings LLP special adviser and UC Berkeley School of Law professor Paul M. Schwartz.

"I don't know how we can keep up at this pace," he said. "For those of us who practice and teach in this field, it's almost scary."

Events overseas continue to create the largest headaches for clients and the most work for their attorneys, as the European Union continues to develop a replacement for its Safe Harbor agreement that previously provided a road map for companies that wish to transfer customer data across the ocean.

The U.S.-EU Safe Harbor Framework was invalidated by the EU Court of Justice in late 2015, forcing the two sides to scramble to create a replacement, the so-called Privacy Shield.

The court ruled that Safe Harbor didn't adequately protect the data of EU citizens, particularly when that information was being transferred across the Atlantic by U.S. technology companies with European users.

The requirements of compliance with the Privacy Shield are not terribly onerous, but the sudden nature of the change and the fact that the new regime could also face legal challenges have created a highly unpredictable situation for multinational corporations, including startup technology companies with limited resources.

The EU and U.S. were forced to replace a regulatory scheme that had been in place for 15 years with the hastily improvised Privacy Shield agreement. The U.S. Department of Commerce began accepting applications for the program from companies in August, giving attorneys a lot of work.

The new regulation requires companies to have agreements with third party contractors they share data with, ensuring they are held to the same standards of protecting sensitive information. It's similar to how a recent update to the privacy provisions in the Health Insurance Portability and Accountability Act, or HIPAA, expanded responsibility for cybersecurity to third party contractors.

That can result in companies having to tear up and rewrite a large number of contracts with their third party contractors.

The new rules also give more power to users whose information is compromised in a data breach. The Department of Commerce is called on to regularly check in with companies about their compliance with the regulations.

The Privacy Shield website indicates that 1,337 organizations have signed up for the program.

Many companies are still going through the process of getting approved under the new rules, said Tanya Forsheit, a partner at Frankfurt Kurnit Klein & Selz PC.

"There were originally more than 4,000 companies Safe Harbor certified," she said. "It's been taking the Department of Commerce a while to review and approve the applications."

In addition to adjusting to the Privacy Shield, which is considered a short-term solution to Safe Harbor's invalidation, companies must also prepare for the new regime, the General Data Protection Regulation, which will go into effect in May 2018 and is still being developed.

Privacy attorneys must spend a lot of time watching arcane political processes playing out in Europe as the new rule is formed, while making sure their clients are in compliance with the current temporary agreement.

Mark L. Krotoski, a privacy and cybersecurity partner with Morgan, Lewis & Bockius LLP, said regulatory sprawl has also been a problem at the state level, where a novel regulation from New York State's department of financial services is creating anxiety among banks and insurers. The new rules are considered to be some of the least flexible guidelines for handling cyberbreach incidents.

Krotoski said the constant process of states leap-frogging each other to create more onerous cybersecurity laws has left clients hoping for a federal law that will pre-empt the web of conflicting state laws that come into play when a company loses customer information.

For companies with any sort of online presence, a single data breach can involve a vast array of regulations, even if it's limited to U.S. customers.

All but three states have some form of individualized data breach requirements at this point. The states vary widely in their instructions for companies that have suffered a breach and some actually contradict the requirements set out by other states.

One state may require a company to notify users immediately of a possible breach, while another will instruct the company to delay notification until after a better understanding of the breach has been ascertained.

"I've helped companies that had all 51 U.S. jurisdictions in play," Krotoski said. "Forty seven states plus Washington, D.C., the Virgin Islands, Guam and Puerto Rico."

Clients hope for more clarity in 2017, but either way, it's a good time to be a privacy attorney.