TEXAS LAWYER

An ALM Publication

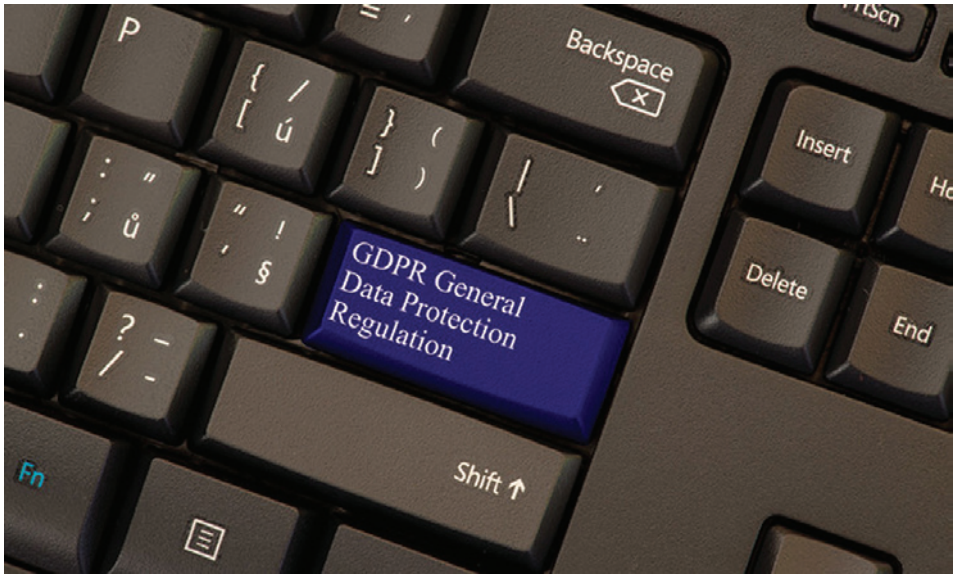
texaslawyer.com | August 30, 2018

Commentary

Managing Cross-Border Data Protection Amid an Evolving Privacy Landscape

BY DEANA UHL

Modern conventions of privacy date back only as far as the industrial revolution, when society adopted the concept of individual and familial privacy, and political and legal visionaries began to introduce the concept of privacy as a right. Since then, and over decades of technological advancement, society's expectations and rules about personal privacy have been on a rollercoaster of change. Today, lawmakers around the world are working to catch up to the vast expanse of digital data and how to govern and limit its commercial use with regard to consumer privacy. The activation of the General Data Protection Regulation (GDPR) in Europe earlier this year, and the emergence of similar laws in China, Latin America, Australia and even some U.S. states, have become the latest evolutions in the long-running privacy paradox.



General Data Protection Regulation.

To date, the extent of enforcement we'll see under GDPR is still in development. The UK Information Commissioner's Office, which is generally considered the most active EU regulator to date, lists **189 actions** on its website and the business sectors impacted span marketing, health, financial services, government and others. Actions include enforcement notices, monetary penalties and prosecutions.

China's Cybersecurity Law, another extensive data protection regulation, went into effect in June 2017. Failure to comply

with restrictions including, protection of key information infrastructure, protection of individual privacy and storage of sensitive data domestically, not transferred outside of China, can lead to serious legal prosecution by the Chinese government, including the suspension or closing of business and fines of up to RMB 1,000,000.

We've also seen some progress in data protection legislation domestically. Last year, the New York Department of Financial Services (NYDFS) issued a cybersecurity regulation — the first of its kind in the U.S. — requiring banks, insurance companies and other financial institutions, including agencies and branches of non-U.S. banks licensed in the state of New York to comply with new guidelines to improve cybersecurity resiliency, and compliance includes retaining personal data only to the extent that it is necessary to executing business needs or for specific regulatory/legal reasons. Another law of note, while still in development, is California's Consumer Privacy Act. As currently drafted, its GDPR-like requirements will apply to organizations that process California residents' personal data and gives data subjects rights over how their data is controlled, including the right to demand that organizations disclose what information they collect on them, to prevent that data from being sold and to take legal action against businesses in violation. Interestingly, a number of recent filings at the FTC complained that enactment of one or more state laws like the CaCPA would result in a patchwork approach of privacy laws in the U.S., which ironically was one of the EU's main drivers for the GDPR.

Alongside the emergence of regulations in recent years, many in the mainstream media have argued that privacy no longer exists. Documentaries and articles in *Forbes*, *Wall Street Journal* and countless other outlets have debated the death of privacy, with some questioning whether privacy matters at all. Despite these discussions, research shows us that consumers do indeed care about keeping their data safe. According to **various studies** from Pew Research, 91 percent of Americans believe that people have "lost control over how personal information is collected and used," and don't understand how their data is collected and used; further, 80 percent of social media users are concerned about access businesses have to their data, and 64 percent think the government should tighten regulation on advertisers. An **NTIA survey** conducted by the U.S. Census Bureau found that "nearly three-quarters of Internet-using households had significant concerns about online privacy and security risks in 2017…[and] about 20 percent said they had experienced an online security breach, identity theft, or a similar crime during the past year."

These consumer concerns, when combined with the cross-border data privacy regulatory developments and the monetary, operational and reputational risks of non-compliance with data protection laws, should be enough to underscore the importance of tackling and maintaining strong data privacy programs. Still, many corporations and their in-house legal teams find themselves stuck without knowing where to begin, or how relevant the regulations are to their business or industry.

A holistic information governance (IG) framework can help corporations create a robust privacy program. IG enables counsel to understand and help lead

initiatives that enable organizations to better understand their data landscape; identify business and cybersecurity risks, provide data transparency to increase competitive advantage and assign accountability and address critical issues. With that knowledge, they can then create the controls and structure necessary to ensure data is protected and managed appropriately. Steps toward a sound program include:

- **Build Cross-Functional Teams**: IG, compliance and privacy programs are often born out of a single function, and eventually become marginalized because they are perceived to not make an impact across the entire organization. When cross-functional teams are aligned, they can address overall risk, not just the risks that apply to a single department.
- **Map Critical Data**: Understanding where critical, personal or sensitive data and assets are stored, and prioritizing security for those first and foremost, helps to arm against the diverse landscape of threats that can compromise privacy.
- **Governance**: The policies established must include built-in enforcement measures. Processes and technologies can be leveraged to track internal compliance with policies and ensure they are sustained across the organization and with third parties.
- **Leverage Training and Incentives**: Employees must receive engaging and customized training to help them understand how to transform habitual activities into practices that align with IG policies.
- **Watch for Emerging Tech:** Technology capabilities are maturing, and we are seeing new tools and features that utilize unstructured data analytics to evaluate risk and identify areas of opportunity in order to make recommendations about where controls should be tightened. Privacy, compliance and IG teams should stay abreast of technology advancements and be prepared to implement tools that can automate some of the most challenging aspects of data management.

Ultimately, data regulation creates an opportunity to leverage data assets for business use and to strengthen the organization's stance on privacy and trust. Counsel that has built a 'privacy by design' IG framework has the foundation in place to demonstrate to its customers, clients and partners that it values their trust and has the means to keep privacy alive across all jurisdictions.

Deana Uhl *is a Senior Director in the FTI Technology practice and is based in Houston. Ms. Uhl provides consulting to corporate clients, with a focus on designing, implementing and enabling change management for information governance, data privacy, data security and e-discovery programs. Ms. Uhl has particular expertise in advising oil and gas companies on the processes and technology to effectively address legal and regulatory matters and improve information quality and life cycle management to support operational excellence.*