BRACEWELL

INSIGHTS

Navigating Domestic and Cross-Border Data Privacy Risks, With Lucy Tyson and Brittney Justice

April 7, 2022

*By: **Matthew G. Nielsen**, **Seth D. DuCharme** and **Lucy Porter***

On this episode of Bracewell Sidebar, ***Lucy Porter*** and ***Brittney Justice*** join hosts ***Seth DuCharme*** and ***Matthew Nielsen*** to talk about data privacy.

Lucy advises clients in a variety of matters related to the structuring and negotiating of services agreements for business process and information technology outsourcing and managed services. Lucy works with clients to develop and implement data privacy solutions that are compliant with global regulations. She has experience working across organizations, including compliance, HR, security, IT and legal. Lucy also has experience in advising clients with the protection, maintenance, licensing and transfer of intellectual property assets, as well as in the prosecution and management of trademark portfolios.

Brittney helps represents clients on cybersecurity and data privacy matters, including privacy litigation, compliance with state and global data privacy laws, and drafting privacy policies and contracts. She also advises on all aspects of data breach incident investigation and response, including directing privileged forensic investigations, coordinating and supporting internal incident response teams, engaging with law enforcement authorities and other federal agencies, and advising senior management on response and risk mitigation strategies.

What is data privacy?

When we say data privacy, we are of course talking about data privacy laws — the set of laws and regulations governing the collection and use of your personal information and the rights that you as an individual may have with respect to that information. They can be generally applicable, which we typically refer to as comprehensive data loss, or they can be specific to an industry. They can vary. They can be broad. They can include consumer data or employee data, or they can be narrow and include just consumers.

Everybody wants their data, their personal information to be private but, from a legal aspect, why does all this matter?

For companies, this matters because of the growing financial and legal risks associated with poor data privacy practices within companies. Threats are growing increasingly sophisticated and pervasive, especially in the world we're living in now and consumers and regulators are calling for more aggressive action from our regulators and from courts as well. We're seeing that being unprepared comes with a hefty price tag. The way companies handle data privacy

and their cybersecurity internally can really become a point of differentiation. Even a source of competitive business advantage if they do this stuff right.

If a corporation is thinking about both cybersecurity and data privacy, does this need to be a Venn diagram? Or can you look at those two issues in isolation?

A component of every data privacy law is going to be your cybersecurity profile. What are you doing to protect your data? Almost every data privacy law hedges. They just say using standard best practices, essentially technical and organizational measures. In the event you have a PII breach, the first thing they're going to look at is, were you protecting the data? So, protecting all of your data should be the goal.

What is GDPR? How is it different from what we have in the United States?

The GDPR, or the General Data Protection Regulation, is the EU's comprehensive data privacy law. It became effective in 2018. It regulates everyone doing business in the EU. It is not industry or jurisdiction specific. It covers everybody — employees, consumers, business to business relationships. It has special provisions for minors, and most importantly it allows for individual member states to make narrower restrictions and to form their own opinions about the activities of either folks in their jurisdictions or the interpretation of the provisions. Why it's really important is because of its extraterritorial applicability. That is why it's driving international privacy. Even if you don't have an office in the EU, you may be subject to the GDPR if you are marketing to selling to residents in the EU.

What should companies be doing from a basic standpoint of starting to build a compliance program?

The first step is you need a multidisciplinary team. You need your legal and your compliance folks involved. You need to have HR involved. You need IT. You've got to have your IT stakeholders involved and thirdly your marketing. A lot of marketing campaigns are going to use personal data because email addresses are going to be personal data. Once you've got your multidisciplinary team engaged, then you can more easily implement a concept called privacy by design, which is going to approach new products, new services, new activities, by looking at it from a privacy perspective and that should, if you're doing that from the very beginning, help you to consider data mapping, consider updates to your privacy policy, things like that.

Have questions about data privacy and compliance? Contact ***Seth DuCharme***, ***Matthew Nielsen***, ***Lucy Porter*** or ***Brittney Justice***.

The opinions expressed in this podcast are those of the speakers and do not necessarily reflect the viewpoint of their institutions or clients.