Corporate Counsel Business Journal
January ▪ February 2019
ccbjournal.com

CCBJ

Managing Data-Privacy Risk And Compliance in a Hyperconnected World

▶ Andrew Shaxted of FTI Consulting is a global data-privacy expert with a background in technology and global risk-management program implementation. We talked to him about what companies can do to manage data-privacy risk and compliance, both from a business standpoint and a technical one.

CCBJ: What is your advice for clients who are concerned about their company's privacy policies and their current technical solutions? What are some best practices?

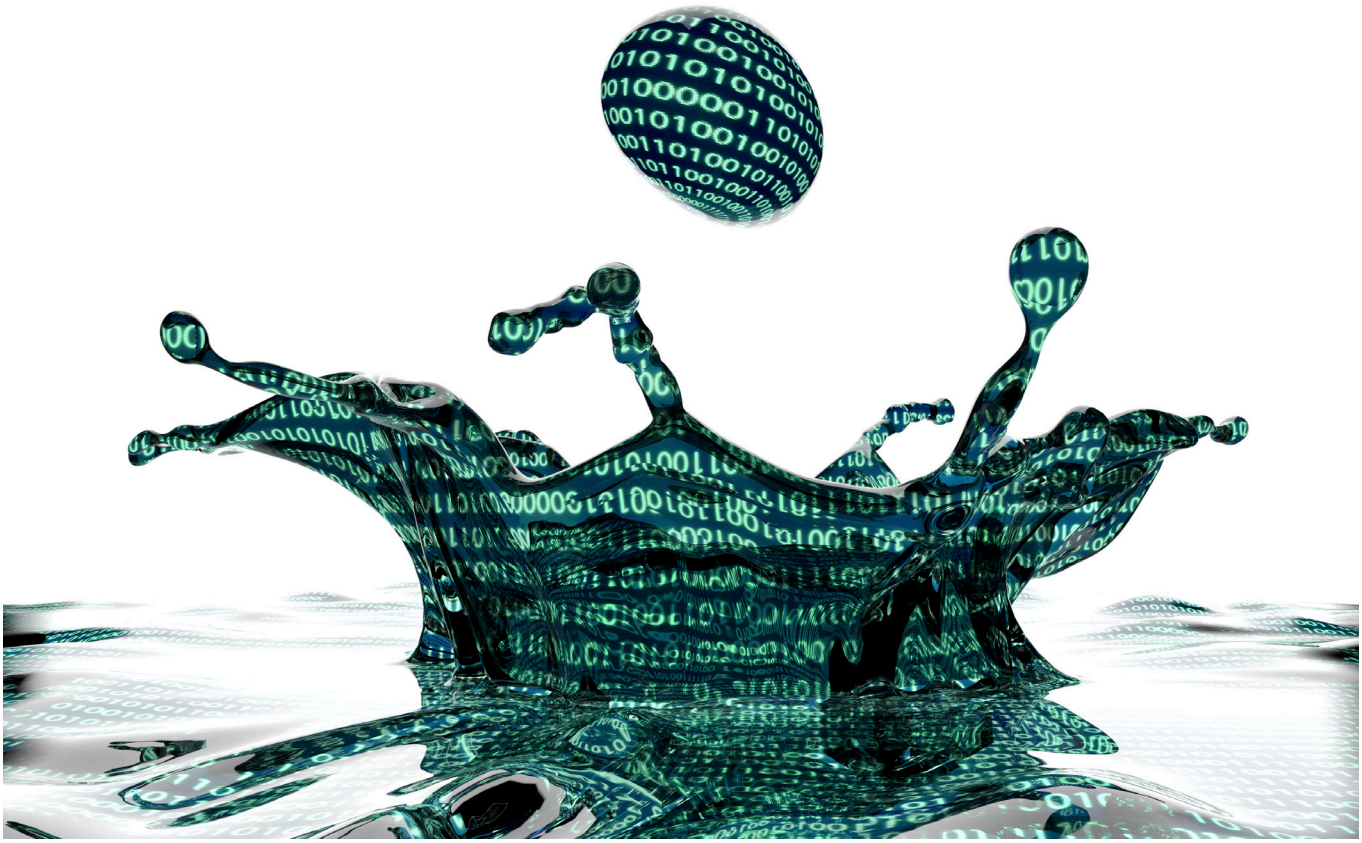
Andrew Shaxted: The privacy policy is just the starting point. It's the documented, defensible position that an organization takes concerning its personal data handling practices and commitment to data privacy compliance. But what's more important to consider is how the policy is being lived out and operationalized at the business level. At the end of the day, the client's concern about the policy may be symptomatic of a general lack of clarity around how the organization actually handles personal data to begin with. Tossing a policy document over the fence for customers to understand or employees to follow is asking for failure. A great tool that I have used in the past and something that has gained more traction since GDPR's effective date is "wikis" and blogs that supplement the policy, providing more clarification and real-world examples. This is especially useful for customer communications but is also helpful for internal employee communications. Going a step further, internal policies and communications must be backed up by a robust training and awareness campaign commensurate to your organization's data privacy risk footprint. Privacy policies are important, but effective privacy risk management is a full change and awareness exercise.

When it comes to technical solutions, it's a similar discussion. While assessment tools, monitoring technologies and automated controls are important for many privacy programs, pain points may quickly surface if the process is poorly understood and improperly executed. Rushing to technology may cause more problems than it solves, so be diligent in developing the strongest processes possible before relying too heavily on technical solutions.

How can companies evaluate their technology and make purchasing decisions that best support their individual privacy needs? Who are the key players in the process?

The privacy-enabling technology market is growing up fast and I expect it will continue to grow and consolidate in the years to come. Even still, like any other enterprise technology, there's no single silver bullet that's going to solve all your company's data-privacy compliance challenges. Taking a step back and having a realistic understanding of what these technologies and tools are capable of doing is an important first step.

The second step is really digging in and working to identify the organization's priority requirements. It can become very confusing if you start having discussions with vendors before truly appreciating and understanding the risks your company is exposed to. If you try to remedy those risks with specific technologies and tools before you've documented – or at least understood and articulated among your key stakeholders – what exactly the risks are, you may end



up buying technology that the company ultimately doesn't have a strategic purpose for.

The stakeholders brought to the table may depend on the organization's size and tech maturity, but the primary factor in determining who the key players are is where the actual privacy risk resides in the organization. Privacy touches so many different areas of a company that it becomes a real challenge to allocate tool investment and ownership to any single function. Privacy enabling technology implementation activities must be cross functional. For companies with significant risk exposure, I would expect to see the Chief Information Officer, Chief Technology Officer, and the Chief Compliance Officer – and where the role exists, the Chief Privacy Officer or equivalent privacy risk owner – sharing executive-level ownership of the requirements gathering, development prioritization and implementation. Additionally, where the business model dictates special technology use cases aligned to a particular function – say marketing or records management – I would expect to see executive-level representation from those areas as well. This is a lot of hands in the pot, but it pays dividends down the road when all critical voices have ownership stake in a successful privacy tool implementation. Understandably, this cross-functional approach may be more easily achieved with smaller organizations but may over-complicate the discussion. The smaller organizations may benefit from a lighter touch approach assuming that their size is indicative of risk posture, which may not always be the case.

How does the growing bring your own device (BYOD) culture play into privacy concerns?

Many applications nowadays allow access to documents and other pieces of information on mobile platforms, which presents numerous risks, simply because those devices may not have the full breadth of security controls that devices located on an organization's security domain would have.

Anytime it's possible to use personal devices to access corporate client data, there needs to be a strategy and policy in place that either allows those devices to

be included on the security domain or else doesn't allow access to corporate information or data if a device is not on the domain.

There are obvious complexities to think about when implementing a policy that permits a BYOD-type situation, especially given the rise of new cloud storage and collaboration tools like Box, Office 365 and others. At the end of the day, BYOD policies create inherent complexity for IT and InfoSec departments. Different device manufacturers have different vulnerabilities that are identified at different times, different operating systems have different vulnerabilities that are identified at different times, and so on. It becomes a very difficult proposition, for larger organizations especially, to enable a BYOD policy without negatively impacting security.

With so much information being shifted to the cloud, what are companies doing to ensure they're compliant with privacy regulations in that area?

When we talk about the cloud, we could be referring to either could-based platforms, applications or system infrastructure tools delivered over the internet. Depending on the specific cloud use case, a company's privacy and information security compliance requirements may vary. Most use cases, however, do share the common risk of transmitting the company's personal data assets to a third party. It is one of the largest sources of anxiety in most cloud arrangements.

Andrew Shaxted is senior director of data privacy at FTI Consulting. He has a background in information security, data-privacy compliance and cloud system implementation. He is a licensed attorney and focuses on management of data-privacy risk and compliance across large enterprises. Reach him at Andrew.Shaxted@fticonsulting.com.

Typically, there are specific things that need to be done in order to comply with the various global data-privacy requirements around third-party collection, storage and management. For example, clearly indicate in the external privacy notice that the company transmits personal data to third parties to carry out standard data management and storage activities. If the company uses cloud systems for its internal HR applications, payroll or benefits administration, the company should also include similar language in the internal privacy policy for employees.

It's important to ensure that the company has appropriate contractual language in place with third-party cloud providers. And just from an operational standpoint, it's important to clearly define the specific points of contact with a vendor, including the specific roles and responsibilities that apply if any sort of incident or issues were to take place. It's also important to have discussions with these cloud service providers, to really understand their system functionality with respect to data-privacy compliance. For example, under GDPR, there's this concept of data subject rights. An individual should be able to pick up a phone and ask an organization to provide access to their personal data, or to stop processing their data or to delete it entirely – "the right to be forgotten" is what it's called. But in order to be able to do that, the organization needs to have perfect command and control over that data, and they need to have the technical capabilities to actually conduct and execute a delete script, or extract a data file that would permit the data subject to have access to their data, for example.

So, it's crucially important for organizations to have these discussions with their third-party cloud vendors, to understand what they are and are not capable of doing.

With GDPR front of mind, how can multinational companies achieve compliance?

The realistic approach isn't so much to march headfirst toward 100 percent compliance. Instead, we recommend taking a risk-based approach, one where organizations consider and understand where the highest risk exists, and where consumer or employee privacy rights are the most exposed. We immediately address those issues first and then navigate through lower-risk items. The order of operation will inform spend and dictate program build and integration priorities. It will also inform technology investments, business process re-engineering and potential program right sizing later down the road. ■