CLIENT ALERT

Compliance in Focus: Working in the Cloud

May.08.2020

The COVID-19 crisis has forced businesses of all kinds to adapt their operations to accommodate remote working for most, if not all, of their workforces. Companies are grappling with ways to adjust their compliance regimes to account for sourcing shifts and other operational challenges, which we have outlined in prior articles.

One of the biggest operational shifts companies today are facing is the rapid acceleration of our migration to cloud computing. Over the past decade, companies have been transitioning away from buying or maintaining their own computing infrastructure to using cloud computing services and applications on an as-needed basis. Now operating on an almost entirely remote basis, companies are increasing their reliance on the Cloud, while others are jumping into the Cloud for the first time. This migration has significant implications for compliance in terms of regulatory recordkeeping requirements, access to data for internal investigations and subpoena responses, and compliance with cross-border data privacy obligations, such as the rigorous requirements of Europe's General Data Protection Regulation (GDPR). Compliance and legal counsel should take stock of the legal and regulatory implications of their company's reliance on the Cloud and consider proactive safeguards they can implement to mitigate the litigation and enforcement-related risks associated with cloud computing.

The CLOUD Act: A Powerful Tool for Compelling Cross-Border Production of Data

Companies using the Cloud to conduct business should take note that cooperation among international regulators is removing obstacles that once frustrated cross-border data sharing.

In March 2018, the United States enacted the Clarifying Lawful Overseas Use of Data (CLOUD) Act to facilitate the sharing of electronic data and communications between the United States and select foreign jurisdictions. Prompting the CLOUD Act was litigation between Microsoft and the U.S. Department of Justice (DOJ) over the extraterritorial reach of the Stored Communications Act (SCA). The United States sought to obtain electronic communications relevant to a narcotics crime investigation that was stored by Microsoft on a server in Ireland. Microsoft refused, arguing in court that the SCA had territorial limitations that prevented the government from compelling production of communications located outside the United States, even when, as was the case with Microsoft, the communications were under the control of a U.S. company subject to U.S. jurisdiction.

The CLOUD Act mooted the dispute between Microsoft and the DOJ by providing a renewed statutory basis for U.S. access to data stored abroad that is in the "possession, custody, or control" of a communications service provider (CSP) subject to U.S. jurisdiction. **In other words, the Act requires that CSPs, such as Amazon, Google and Microsoft, comply with U.S. law enforcement requests for data under their control, regardless of where the data is located.**

The CLOUD Act also authorizes the U.S. to enter into executive agreements with select foreign governments that could potentially transform cross-border data sharing. Absent these agreements, foreign data is accessed through processes established by Mutual Legal Assistance Treaties (MLATs), which allow law enforcement agencies in one country to engage their

foreign counterparts for assistance in accessing data. The foreign authorities serve as a conduit, reviewing the request, determining if it violates their laws and, provided it does not, transmitting the data to the requesting government. It can take foreign authorities more than a year to successfully navigate the MLAT process with the United States, which requires multiple layers of DOJ review. It can take even longer for the U.S. to access documents abroad, if it is able to do so at all. The CLOUD Act allows parties to an executive agreement to side-step this process and access foreign-based data on a more expedited basis. It is contemplated that under executive agreements, CSPs can comply with document requests from the foreign government without the need for approval or review by their local authorities and without concern that providing the data will violate local law.

The first of these executive agreements—between the United States and United Kingdom—is set to take effect later this year, and others between the United States and Australia and the United States and the European Union are underway. With nearly all Western nations negotiating expedited international data sharing, understanding the CLOUD Act and its impact is essential for companies doing business in the Cloud.

What Legal & Regulatory Risks Does the CLOUD Act Raise?

Particularly in light of the potential for thorny conflicts between U.S. enforcement demands and local data privacy protections, the CLOUD Act has the potential to raise risks spanning from litigation related to data privacy complaints by customers and third parties to protracted negotiations and potential litigation over enforcement demands for documents and information. Below are three critical considerations for companies, their compliance officers and counsel, as we all transition further into the Cloud.

1. Possession, Custody, or Control

As the Microsoft case shows us, the location of cloud servers, while important, is not determinative. When it comes to access by regulators, often the key consideration is who is in "possession, custody, or control" of the data. Companies should assess which vendors, partners or CSPs could arguably have "possession, custody, or control" of their data. Once parties with such access are identified, companies should consider contractual and technological safeguards to avoid potential conflict with data privacy restrictions, privacy obligations or expectations that may run to third parties. Such safeguards could include representations and disclosures concerning the protection of data in the company's possession and the potential for regulatory demands as well as contractual provisions clarifying third parties' control over particular data and any limitations to that control.

2. Location

Although not determinative, the location of the servers on which the Cloud's data is stored can be very important, particularly in light of the CLOUD Act and cross-border cooperation agreements set to take full effect later this year. Knowing where your data is stored can help inform your understanding as to which regulators are likely to request access, either directly or via cooperation agreements. Knowing this may impact which data companies voluntarily share, for instance, with partners, vendors or in the context of cooperating with a government regulator. But perhaps more importantly, it can help companies preempt any conflict of laws issues and take a thoughtful and informed position as to how to respond in the event of a regulatory request (either directly or through a third party), thereby mitigating the risk of having to navigate conflicting obligations to multiple jurisdictions.

3. CSP Agreements

Finally, this is an opportune time to revisit your agreements with your CSPs and ensure that they account for recent regulatory developments. For instance, companies should note that the Agreement between the United States and United Kingdom does not require a CSP to notify its client (or the data subject) that it has received a document request from a regulator. Whether notice is provided may therefore depend on the terms of the agreement between the CSP and its client. This notice, or lack thereof, could have important implications on a company's ability to intervene or limit the scope of the request on the basis of attorney-client privilege.

None of this is to suggest that companies should plan their data storage and access to avoid legitimate document requests from regulatory authorities. Rather, companies should take stock of where their data is stored, who has access to it, and what disclosures have been made to data owners because the guideposts that companies, their vendors, and their customers once relied on to evaluate data privacy risks are changing. Prudent companies will have the foresight to carefully assess the risks that cloud storage and third-party data access may raise and will craft safeguards and disclosures to mitigate those risks today and avoid a sticky situation tomorrow.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Michael D. Mann
Partner – Washington, D.C.
Phone: +1 202.261.2990
Email: mmann@crowell.com