

INSIGHTS

Hey, You, Get Off Of My Cloud – New DOJ Approach To Remote Data Storage

January 9, 2018



Last month, the Department of Justice’s Computer Crime and Intellectual Property Section, Criminal Division (“CCIPS”) issued new guidance advising prosecutors seeking enterprise customer data stored “in the cloud” to attempt to collect responsive information from the enterprise first, instead of serving information requests directly on the enterprise’s cloud data service provider. The guidance represents a departure from recent investigation trends to serve information requests directly on the cloud data service provider to the exclusion of the impacted enterprise and reflects a recognition by DOJ of the limits and inconvenience of data extraction at the cloud storage level. The new approach is likely welcomed by cloud data service providers. For example, Microsoft has been engaged in a long-term customer privacy rights challenge with the government and Amazon.com recently disclosed that in the first half of 2017, it received a record number of requests for information belonging to customers of Amazon’s cloud computing service. CCIPS’s guidance also serves as a warning to enterprises that rely on their cloud data service provider to respond to information requests. Enterprises should be aware of where and how their data is stored, and be prepared to respond to a direct data request regardless of where that data is stored.

CCIPS's recommendations reflect the practical considerations of cloud data services used by enterprises (defined as companies, academic institutions, non-profit organizations, or the like but not individuals), and the challenges that cloud data storage poses for law enforcement officials conducting investigations. The government articulated that obtaining information directly from cloud data service providers typically takes longer, results in overly broad information dumps, and there is varied level of ability and skill among cloud providers to respond to targeted information requests especially if the information stored is encrypted by the enterprise. Additionally, some cloud data service providers act only as storage facilities allowing the enterprise to control access, deletion, preservation and extraction.

In an effort to improve the efficiency of investigations by avoiding delay and overly broad responses to information requests, CCIPS suggests that prosecutors "should seek data directly from the enterprise, if practical, and if doing so will not compromise the investigation." Before going directly to the enterprise, prosecutors are instructed to consider:

- whether the enterprise or the cloud data service provider is the best source for the information sought;
- whether there is an appropriate contact at the enterprise who can secure the data such as a general counsel; and
- whether approaching the enterprise increases the risk that an employee of the enterprise will purposefully destroy the data.

CCIPS further recommends that the prosecutor should consider whether to, before approaching the enterprise, first request that the cloud data service provider preserve the data.

The guidance recognizes that certain circumstances weigh against going directly to the enterprise. For example, if the enterprise itself is engaged in criminal activity, there is evidence that the enterprise would not willingly comply with the request, or there simply is not a trained or appropriate individual at the enterprise to facilitate response to the information request.

DOJ's approach to investigations in the wake of the ever-changing technological landscape, continues to evolve. For some, the new guidance represents a positive step toward transparency and engagement between DOJ and businesses to facilitate law enforcement investigations. For others who rely on cloud data services for email and other information storage, CCIPS's guidance is a gentle nudge to consider how effective it might be, or whether it has the right personnel and technology to responsibly collect data and provide timely and complete responses to a direct request from the government.