Seeking Enterprise Customer Data Held by Cloud Service Providers

Computer Crime and Intellectual Property Section, Criminal Division
U.S. Department of Justice
December 2017

Individuals and enterprises are increasingly moving their data to the "cloud." Cloud-based solutions, by which entities contract for storage and other services from providers, can reduce information technology infrastructure costs, increase resiliency, and improve data availability for mobile workers. At the same time, such solutions can pose unique challenges in criminal investigations because they can implicate information stored by individuals and organizations who are not subject to the investigation. For example, the government may seek information belonging to a company, government agency, university, or other enterprise (rather than an individual person). The entity itself is not a subject of the investigation, and the information sought is but a small subset of the entity's information stored in the cloud. Because these instances will continue to arise in the future, we have identified recommended practices for dealing with such situations, based on recent experience working with providers and prosecutors seeking an entity's information stored with a provider of cloud services. In general, as explained below, prosecutors should seek data directly from the enterprise, rather than its cloud-storage provider, if doing so will not compromise the investigation.

By "enterprises", we mean companies, academic institutions, non-profit organizations, government agencies, and similar entities that pay service providers to store electronic communications and other records. In the past ten years, there has been a notable change in how enterprises manage employee email and other types of electronic records. Previously, enterprises commonly owned and operated their own servers for email and data management, which were physically located on the enterprise's own property. Today, enterprises increasingly use cloud service providers to manage email for employees (or students, contractors, and any other individuals associated with the enterprise), as well as for other types of information. Under this arrangement, the enterprise pays the cloud service provider to host its email accounts and data. Although the enterprise's email addresses still bear the enterprise's domain name (that is, for example, they end in "@company.com"), the service provider stores its content and helps manage access and security for the domain.

The transition to cloud storage has implications for how the government obtains the contents of email accounts (and other data contained in cloud storage) during a criminal investigation. Prior to the advent of widespread cloud services, prosecutors had to approach a company or similar enterprise directly for electronic data stored on servers located on an enterprise's premises. The information was obtained through grand jury subpoenas or other types of information requests or through targeted search warrants. Since the advent of cloud computing, however, prosecutors have the legal authority to compel the enterprise or a cloud service provider to produce the data. Compelling the cloud provider to produce the data when the enterprise is not the potential target, however, comes with potential downsides, including the lengthier time often required to obtain the information useful to an investigation by seeking enterprise data from a cloud provider.

The nature of cloud storage and processing services can differ greatly from provider to provider—and even among service offerings by the same provider. Depending on the type of service offered, providers may lack the appropriate tools to preserve or disclose data on particular employees or other individuals within the enterprise. A cloud email provider may provide primarily back-end storage and web-based applications to an enterprise, allowing the enterprise to handle administration such as individual account creation, deletion, preservation, and disclosure. In such cases, the cloud provider may lack the necessary tools to readily extract data relating to an individual employee. Moreover, a provider will not always have access to all possible data. For example, the enterprise might encrypt data on its own systems before transmitting to their cloud provider.

Because of these and other potential complications, prosecutors should seek data directly from the enterprise, if practical, and if doing so will not compromise the investigation. Therefore, before seeking data from a provider, the prosecutor, working with agents, should determine whether the enterprise or the provider is the better source for the data being sought. While cloud services have changed the location of the servers storing enterprise data, in many cases the enterprise maintains primary control over the data. If an investigation requires only a subset of data—for example, the email accounts of a small group of employees, or data relating to a particular group of transactions—approaching the enterprise will often be the best way to get the information or data sought, while avoiding over-collection, which can be a challenge in many investigations. In those cases, identifying an individual within the enterprise who is an appropriate contact for securing the data is often the first step. In many enterprises, this will be the general counsel or legal representative. Counsel typically understand law enforcement needs and—perhaps more importantly—understand the importance of preserving enterprise data that has been identified as relevant to an ongoing law enforcement investigation. Working with counsel and the enterprise's information technology staff, law enforcement can identify and seek disclosure of relevant information. This approach also gives the counsel the opportunity to interpose privilege and other objections to disclosure for appropriate resolution, and parallels the approach that would be employed if the enterprise maintained data on its own servers, rather than in the cloud.

Approaching the enterprise directly does comes with the potential danger that an employee in the enterprise, alerted to the government's investigation, will improperly destroy data. Because of this risk, investigators should consider whether to seek preservation of enterprise data by the provider under 18 U.S.C. § 2703(f) to protect the investigation. If the provider can undertake preservation prior to law enforcement seeking evidence from the enterprise, law enforcement is in a better position to ensure that data sought by investigators is not inadvertently or intentionally destroyed. The knowledge of a provider-made backup may itself be a deterrent to those who would risk additional culpability by attempting to hide or destroy relevant data.

In other cases, however, prosecutors or agents have justified reasons for not approaching the enterprise directly, at least initially. If an enterprise is essentially devoted to criminal activity—for example, a small medical practice suspected of engaging in massive Medicare fraud—there may not be a trustworthy individual to approach. If law enforcement has developed reasons to believe that the enterprise will be unwilling to comply or if the enterprise itself is principally devoted to criminal conduct, seeking disclosure directly from the cloud provider may

be the only practical option. This is similar to the situation in non-cloud contexts where law enforcement is concerned that the enterprise will destroy evidence if served with an ordinary subpoena, and therefore seeks a forthwith subpoena or search warrant for the business premises.

Other practical considerations might also leave the government with no choice but to seek disclosure directly from the provider. Law enforcement may be concerned that the enterprise's staff is not capable of isolating and disclosing the necessary information, and that the cloud provider is in the best position to do so. Law enforcement might be unable to find a trustworthy point of contact (or, perhaps, any point of contact) at the enterprise. Disclosure of the investigation at a sensitive stage might put a cooperating witness in danger. In our experience, providers understand that these situations may exist and will work with law enforcement to address these concerns.

Additional factors to consider before seeking disclosure directly from the provider include:

- The purpose for which the communications or records are sought and their importance to the investigation or prosecution;
- The extent of law enforcement's ability to obtain the communications or records from the enterprise;
- Whether the enterprise is a subsidiary of a larger institution and, if so, whether the government is aware of a contact at the parent institution;
- The extent to which the enterprise is technologically capable of providing the communications or records;
- The risk of an adverse result for the investigation if the enterprise becomes, or individual(s) who would be the logical contact at the enterprise become, aware of the government's investigation, taking into account the possibility of mitigating this risk through a preservation letter to the service provider or instructions to the enterprise not to notify the target of the investigation;
    - Adverse results can include those listed in 18 U.S.C. § 2705: endangerment of the life or physical safety of an individual; flight from prosecution; destruction of or tampering with evidence; intimidation of potential witnesses; or otherwise seriously jeopardizing an investigation or unduly delaying a trial.

In general, CCIPS has found many cloud providers are sensitive to the concerns of investigators and prosecutors—including concerns about jeopardizing the integrity of an investigation. For example, where cloud customers have designated a point of contact in the enterprise who can be relied on to respond to government requests, or be notified of their existence, without jeopardizing the investigation, cloud providers can often redirect law enforcement personnel to that resource. Accordingly, in such cases, consideration should be given to whether the request should be redirected to the enterprise, as well as whether any protective order can be narrowed to permit the provider to notify an appropriate official at the

enterprise without posing a risk to the integrity of the investigation. To the extent that CCIPS can help facilitate these conversations, we are happy to assist offices through their Computer Hacking and Intellectual Property coordinators or, in national security matters, the National Security Cyber Specialists in conjunction with the National Security Division. CCIPS duty attorneys are available at 202-514-1026.