Data in Rest vs. Data in Motion

Data sought by law enforcement can be generalized into two broad categories: data in motion and data at rest. Data in motion refers to information that is actively in transit from one location to another, such as an exchange of phone calls, texts, and emails, or data transferred from a local device to a cloud storage device. Data at rest refers to information that is stored on a laptop, hard drive, or other storage mechanism. Contrary to data in motion, data at rest is not actively moving among devices or networks.[i]

With the proliferation of digital devices and platforms for internet-enabled communication, technology companies are often the gatekeepers of all electronic data.

Historically, law enforcement could gain access to user data through a straightforward legal process. Under the 1986 Stored Communications Act (SCA), technology companies (and Internet Service Providers) were compelled to relinquish data upon the receipt of a lawfully issued warrant. However, now many American tech companies have chosen to store user data on servers housed overseas. The legislation, drafted over 30 years ago, was proposed long before U.S. based companies began storing emails, files, and other data on foreign servers and so does not adequately address this issue.

Microsoft Decision

In a 2016 court case, *Microsoft Corporation v. United States*, Microsoft's lawyers argued that the SCA did not grant U.S. law enforcement the authority to seize foreign stored data without approval from the foreign country's government. The Second Circuit determined that the SCA does not give U.S. judges extraterritorial authority, and therefore they cannot issue search warrants that extend beyond American soil. As a result, the government, even with a warrant, cannot require Internet Service Providers based in the United States to relinquish data that is stored overseas. [ii]

This verdict, otherwise known as the *Microsoft* decision, poses challenges for law enforcement officials seeking overseas data for criminal prosecutions. In cases where U.S. based technology companies elect to house their data in overseas locations, the foreign-stored data is not subject to U.S. judicial orders.[iii]

Mutual Legal Assistance Treaty (MLAT) Process

Because police agencies cannot directly serve international sources, they must utilize the MLAT process to ensure that legal requirements in each country are followed.[iv] MLATS are agreements between two or more countries that "allow prosecutors to enlist the investigatory authority of another nation to secure evidence — physical, documentary, and testimonial — for use in criminal proceedings by requesting mutual legal assistance."[v] To obtain assistance pursuant to MLAT, there are four steps that law enforcement must follow:

1. Obtain a model request for the relevant MLAT Agreement from the Office of International Affairs (OIA).
2. Prepare a draft request and submit to OIA for approval.
3. Revise as directed by OIA and submit to DOJ for authorizing signature.
4. Obtain a translation of the request, if necessary, and submit to OIA.

After these steps are completed, the OIA files the request with the foreign authority in the respective country. The foreign authority is now bound, under the country's MLAT with the United States, to aid the investigation.[vi]

Implications for Law Enforcement

In our increasingly interconnected world, nearly all crimes have a digital component. As police encounter digital data through many different types of devices (e.g., cell phones, computers, FitBits, GPS systems), investigators are using digital evidence to enhance investigations. In many cases, police rely on ISPs to provide this information.

- With the proliferation of digital data, ISPs are increasingly globalizing data storage. Even if a client lives in the United States, the ISP may elect to store the user's account information on an overseas server. Which means, the police must use the cumbersome MLAT process, which poses a number of investigative challenges, including: **Loss of evidence**: The process for obtaining overseas data can be slow and time consuming. During the time it takes to obtain search warrants, work with ISPs, and navigate the MLAT process, data could be lost or deleted if it is not secured. As a result, law enforcement officials have expressed concern over the potential loss of evidence.[vii]
- **Scattered data**: ISPs that elect to store data overseas often disseminate information among numerous servers. This means that a single user's data could be spread across multiple servers, possibly in several different countries. In such cases, law enforcement must utilize the MLAT process for each country in which data is stored, even if it is tied to the same user. This tedious and time-consuming process can cause serious delays for investigators. [viii]

Resources

Within the Department of Justice, the Computer Crime and Intellectual Property Section (CCIPS)[ix] assists law enforcement with the preservation of overseas data. A request for preservation of overseas data should be made to the email address 24.7@usdoj.gov. CCIPS personnel will forward the request to contacts in the requested country. They also operate a 24/7 service line in case of emergencies. Law enforcement personnel can call the duty line at (202) 514-1026 and ask for the duty attorney. Calls made to the duty line outside of normal business hours are routed through the Justice Command Center to the on-call duty lawyer.

The National Domestic Communications Assistance Center (NDCAC) also provides valuable resources for law enforcement official seeking data from ISPs. NDCAC maintains a database with documents to aid in data requests to ISPs. These files include point of contact information and search warrant templates for over 100 applications. [x]

---

[i] Lord, N. (2017, July 27). What Is Data Encryption? Retrieved from https://digitalguardian.com/blog/data-protection-data-in-transit-vs-data-at-rest

[ii] *Microsoft Corp. v. United States*. (2016). Retrieved from https://law.justia.com/cases/federal/appellate-courts/ca2/14-2985/14-2985-2016-07-14.html

[iii] Ibid.

[iv] Goodison, S., Davis, R., & Jackson, B. (2015). *Digital Evidence and the US Criminal Justice System*. Retrieved from https://www.ncjrs.gov/pdffiles1/nij/grants/248770.pdf

[v] Rush, M., & Kephart, J. (2017, January 20). *Lifting the Veil on the MLAT Process: A Guide to Understanding and Responding to MLA Requests* [Scholarly project]. In *K & L Gates*. Retrieved from http://m.klgates.com/files/Publication/669681d7-12d7-451e-8240-a33cf67c959f/Presentation/PublicationAttachment/ec5fc22d-3e3c-4607-bcb3-f4e99e3f59b4/GE_Alert_01202017.pdf

[vi] Ibid.

[vii] Ibid.

[viii] Ibid.

[ix] See https://www.justice.gov/criminal-ccips

[x] See https://ndcac.fbi.gov/