POLICE EXECUTIVE RESEARCH FORUM

The CLOUD Act

and Implications for Law Enforcement

Overview

The passage of the CLOUD Act (short for Clarifying Lawful Overseas Use of Data) seemingly resolved the Microsoft case[i] and was considered a victory for law enforcement in their quest to lawfully obtain data housed in overseas servers by U.S. based companies. Here we provide an overview of the CLOUD Act and the practical implications for law enforcement, followed by a discussion of the challenges presented by Europe's newly enacted General Data Protection Regulation (GDPR).

Problems Facing Police Extraction of Data Prior to the CLOUD Act

Prior to the passage of the CLOUD Act, police were restricted in their ability to obtain data stored in overseas servers when conducting criminal investigations. As a result of the 2016 Second Circuit court case, *Microsoft Corporation v. United States,* the government, even with a warrant, could not require Internet Service Providers based in the United States to relinquish data stored overseas.[ii] Law enforcement was therefore forced to undergo the lengthy Mutual Legal Assistance Treaty (MLAT) Process, which often prevented agencies from gaining access to the communications needed for their investigations in a timely and effective manner.[iii]

The Microsoft case revealed how outdated US laws were regarding access to remote data storage. The ruling was made based on the 1986 Stored Communications Act (SCA), which did not even account for cloud-based data, let alone data stored on servers in different countries.[iv] As a result, law enforcement leaders advocated for legislation that would address their current technological and investigate needs and mitigate the challenges posed by the Microsoft case.[v] A legislative solution was reached on March 23, 2018, when the CLOUD Act was signed into law.

What the CLOUD Act Addresses

The CLOUD Act has three major components. The first is to make clear that Chapter 121 of title 18, United States Code, describing the process by which officers can gain access to stored wire and electronic communications, applies to information that is stored on servers located outside of the United States. This provision ensures that, in a scenario such as the Microsoft Case, a U.S. based company could not use the fact that the servers are overseas as a justification for noncompliance.[vi]

The second component involves data that is stored overseas and concerns subjects who do not reside in the United States and who are not United States Persons.[vii] For these cases, the CLOUD Act mandates that judges weigh the benefits that such evidence would provide against the importance of other

factors, such as the interests of the foreign government, the ability to get the same information by other means, and possible penalties on the provider if they release the data.[viii]

Finally, the Act gives the executive branch the authority to make certain types of agreements regarding access to data with foreign governments, as long as the foreign governments demonstrate a commitment to rule of law and privacy protections, among other provisions. Any agreement also must ensure that foreign governments cannot use the data to target US Persons either directly or indirectly, and they cannot use the data to target what the United States would consider protected free speech.[ix]

Implications for Law Enforcement

The CLOUD Act gives law enforcement the tools they need to extract relevant information for the investigation in cases involving electronic communications by U.S. residents stored in overseas servers by U.S. based companies. In these cases, courts can issue warrants for the communications regardless of whether they are stored on servers outside of the United States. This provision streamlines the evidence gathering process for many agencies.

In cases involving non-US residents the implications of the act are less clear. The warrant must go through a lengthier court review process, which is further complicated by the fact that many countries do not yet have treaties in place with the United States to govern access to data. So although the Act paves the way for more efficient data extraction by allowing the executive branch to make these treaties, the full effects on law enforcement in these cases have yet to emerge.[x]

Issues on the Horizon: Europe's General Data Protection Regulation (GDPR)

The European Union enacted the GDPR in May 2018. This regulation puts limits on the transfer of data from the EU, including a provision regarding foreign court orders. Article 48 states that, "Any judgement of a court… of a third country requiring a controller or processor to transfer or disclose personal data may only be recognized or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty…"[xi]

While this regulation appears to conflict with the CLOUD Act, it also includes provisions that could mitigate such concerns, such as an exception to article 48 that allows transfers that are "necessary for important reasons of public interest" or "necessary for the purposes of compelling legitimate interests pursued by the controller,"[xii] which could be interpreted as including requirements under the CLOUD Act.

Although the complete international legal landscape has not yet become clear, the CLOUD Act is an important step towards modernizing United States data laws and could prove to be a vital tool for law enforcement officials seeking to gain more efficient access to cloud-based communications.

[i] For more information on *Microsoft Corp. v. United States, see* PERF's document on the LECC entitled, "Law Enforcement & Overseas Data". http://www.iacpcybercenter.org/wp-content/uploads/2017/11/Overseas-Data.pdf

[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] 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

[iv] *Microsoft Corp. v. United States*.

[v] It should be noted here that the Second Circuit decision was under review by the Supreme Court at the time that the CLOUD Act was passed. This review makes it unclear whether the Court would have granted district courts the authority to issue warrants on servers in different countries. The CLOUD Act made the discussion mute, and the Supreme Court case was vacated soon after its passage.

[vi] Consolidated Appropriations Act of 2018, HR 1625, 115th Cong. (2018). Retrieved from https://www.congress.gov/bill/115th-congress/house-bill/1625/text

[vii] Under the act, a United States Person is classified as a US citizen, an alien lawfully admitted for permanent residence, or a US corporation/association.

[viii] Consolidated Appropriations Act of 2018.

[ix] Ibid.

[x] Ibid.

[xi] The General Data Protection Regulation (GDPR) (EU) 2016/679, Art 48. Retrieved from https://gdpr-info.eu/art-48-gdpr/

[xii] The General Data Protection Regulation (GDPR) (EU) 2016/679, Art 49. Retrieved from https://gdpr-info.eu/art-49-gdpr/