‘C.L.O.U.D.’s On the Horizon: How Law Enforcement Electronic Data Requests Are Going Global

Although they each may have their own wrinkles, new executive agreements will assuredly increase the volume of content requests from foreign governments.

By **Chris Ott, Davis Wright Tremaine** | October 28, 2019

Companies storing or moving large quantities of digital information routinely encounter subpoenas, court orders and warrants from United States law enforcement for subscriber and related data and records. However, the realities of cybercrime and recent under-publicized diplomatic activities could dramatically increase the volume of incoming requests from abroad.

Cybercrime often involves a crime in one country—a hack of a school teacher’s email account in the United Kingdom, for example—but the evidence of the crime often physically resides on servers in another country, such as malware and login records maintained by a social media or online company in California. However, law enforcement agencies investigating multi-country crimes are often bound by the geographic limits of their jurisdictions or must rely on slow diplomatic channels, such as mutual legal

assistance treaties (MLATs), to request and obtain the evidence that they need. This slow process necessarily restricted the number of international requests received by U.S. companies.

The 2018 Clarifying Lawful Overseas Use of Data Act (CLOUD Act) authorizes the U.S. to enter into executive agreements with foreign governments to facilitate law enforcement access to cross-border data. The U.S. and the U.K. signed the first CLOUD Act Executive Agreement on October 3, 2019. Now, law enforcement agencies in either country can, according to the U.S. Department of Justice, "demand electronic evidence directly from tech companies based in the other country, without legal barriers." The Agreement cannot take effect until the legislatures of the respective countries have had six months to review the agreement (April 2020). However, more are coming: the European Union began discussions for an executive agreement and, on October 7, the U.S. and Australia announced that their own executive agreement negotiations. With these agreements on the way, the privacy protections built into the Act and the U.S./U.K. Executive Agreement provide some guidance as how those changes will affect companies.

Scope

Article 1 of the Executive Agreement specifies that any "private entity" that "provides to the public the ability to communicate, or to process or store computer data" or "processes or stores" data for those public-facing private entities, are potential recipients of UK law enforcement process. While necessarily focused on telecommunications and internet service providers, the expansive nature of modern data and the broad definition of "communication" means many companies in the information and data economies can expect cross-border data requests.

The covered data includes communication content, computer data, traffic data, metadata, and “Subscriber Information.” Subscriber Information, as defined, echoes the Stored Communications Act, which lists the information that can be requested by U.S. law enforcement via subpoena. As discussed below, requests for the U.K. persons’ communications content may be subject to a lower standard than required under U.S. law.

Issuance and Oversight

Judicial review and oversight of these cross-border data requests is not simple. Executive Agreement Article 5 specifies that the cross-border orders must be reviewed and certified as lawful by a “designated authority.” For U.K. law enforcement requests to U.S. companies, the U.K. Home Secretary designates their authority and the order must then be reviewed by U.K. judges or magistrates. Thus, U.S. companies will now receive orders from U.K. judges that will carry the force of law and the inverse is true for U.K. companies. The orders must certify in writing that the order is based upon “articulable and credible facts.”

Under existing U.S. law, the “articulable and credible facts” standard set forth in the agreement would likely suffice for orders requesting subscriber information and records, but not the content of communications. Indeed, even certain con-content information would require probable cause. In the context of cell site location data (which possesses no content), the Supreme Court found that a warrant was also required, and noted that the requirements for basing an order on “articulable and credible facts” falls “well short of the probable cause required for a warrant.”

Companies who are issued one of these new orders can appeal to the issuing “designated authority” for clarification. However, this “clarification” will not

change the potentially awkward fact that U.S. companies will be faced with U.K. orders certifying compliance with U.K. laws but not U.S. laws (or the reverse situation). If the objections are not resolved by the issuing designated authority, the company can contact its own designated authority. This is where things get even more complicated. Article 5 contemplates that the two governments will negotiate but that the provider's own designated authority decides. Therefore, a U.S. designated authority will have ultimate authority over a request to a U.S. company.

The Executive Agreement and CLOUD Act are largely silent on what a "Designated Authority" actually is. However, the Articles 1 and 5 of the Executive Agreement provide that: (1) the "issuing party" will be a law enforcement agency; (2) judges or magistrates will review data requests by the issuing party; and (3) "Designated Authorities," who are distinct from either the issuing party or the judge, and selected by the U.S. Attorney General or the U.K. Home Secretary, preside over it all. Given similar existing designations in the United States Attorneys Manual, the Designated Authority may be a subpart of the Department of Justice. In certain immigration circumstances, the "designated authority" is the State Department. Whomever or whatever entity is selected, the Designated Authority is unlikely to be an independent court and cross-border data requests may have little substantive legal review.

Data Targeting and Use Limitations

According to the executive agreement, U.K. law enforcement cannot seek the communications content of U.S. persons (which, as discussed above, would require a warrant in the U.S. based on probable cause). Requests must be targeted to specific accounts, addresses or persons. Therefore, the CLOUD Act cannot be utilized for "bulk surveillance." However, most online data is

pseudonymous and U.K. law enforcement may not know the location, name, or address of the target until they receive the data. Instead, they only know the cookie, online persona, or other alphanumeric identifier. While the U.S. and U.K. must implement protections for incidentally collected data via this CLOUD Act process, each company will have to consider its own appetite for these types of mistakes. Companies may have to consider prophylactic challenges in cross-border requests or risk good faith violations of peoples' privacy.

Article 8 of the Executive Agreement provides that the U.K. need not provide evidence for use in a U.S. death penalty cases and may even veto its use post hoc, as needed. The U.S. has similar veto power obviating production in cases that raise free speech concerns. These veto powers appear to be novel, although they may become standard for the upcoming Executive Agreements.

Conclusions

This will likely be the first of many Executive Agreements that will issue in the coming years. Although they each may have their own wrinkles, these agreements will assuredly increase the volume of content requests from foreign governments. These agreements will also have tricky oversight and review frameworks. Moreover, the data use exclusions included in each agreement may provide interesting insight into which rights are most important to each country. Finally, while decryption was expressly excluded from the agreement, that issue and potential conflicts with the EU "e-evidence Rule" must be watched closely.

Chris Ott, CIPP/US, advises industry-leading organizations in sensitive cyber incidents, national security matters, white-collar investigations, government enforcement actions, and high-stakes litigation. Chris has served as an influential law enforcement official for multiple administrations, led some of the largest white-collar investigations in United States Department of Justice (DOJ) history, won more than 30 trials as a first-chair litigator, and spearheaded some of the DOJ and the SEC's first successful cyber investigations. Chris, who is a partner in the Washington, D.C. office of Davis Wright Tremaine, can be reached at ***chrisott@dwt.com****.*
