What You Should Know About The 24/7 Cybercrime Network

By **Chris Ott** (June 28, 2018, 1:40 PM EDT)

Chris Ott

Sophisticated companies are used to responding to grand jury subpoenas, court orders and search warrants. Internet service providers have dealt with orders under 18 U.S.C. § 2703(d) or mutual legal assistance treaties. The 24/7 Cybercrime Network adds a new wrinkle for preserving electronic evidence. The Clarifying Lawful Overseas Use of Data Act, or the CLOUD Act, passed as part of the federal government's spending bill in March 2018, also governs the preservation and production of certain electronic evidence. The waters were further muddied by the European Commission's new "e-evidence" rules, which were proposed on April 17, 2018. Notwithstanding, as discussed below, the 24/7 Cybercrime Network will remain a tool used by foreign countries in obtaining electronic evidence from companies in the United States.

The G7 and the Fight Against International, High-Tech Crime

Seven major countries make up the Group of Seven: the U.S., Japan, Germany, the U.K., France, Italy and Canada.[1] The heads of state or government of the G7 gather for annual summits to discuss important domestic and international economic and political issues. One of these summits happened the weekend of June 8, 2018, in Canada.[2] The G7 also creates task forces and working groups on certain matters such as transnational organized crime.[3] As part of that effort, the G7's "Roma-Lyon Group's High-Tech Crime Subgroup" operates the G7 24/7 Cybercrime Network.[4]

The 24/7 Cybercrime Network includes more than 70 countries. The network exists primarily to "preserve digital evidence for subsequent transfer through legal channels."[5] It was created in December 1997 with the following statement of purpose:

With regard to high-tech crime, we must start by recognizing that new computer and telecommunications technologies offer unprecedented opportunities for global communication. As nations become increasingly reliant upon these technologies, including wireless communications, their exploitation by high-tech criminals poses an ever-greater threat to public safety.[6]

Following up on that, the member countries created a single point-of-contact available to all other member nations, 24 hours per day and seven days a week. The purpose of the network is to permit the countries to quickly and efficiently preserve evanescent data in other member countries. Months after the preservation order is issued, an MLAT request would issue to gain custody of and transfer the data. This combination of fast preservation orders and slower diplomatic transfer requests has sometimes been called a "fast freeze and a slow thaw." The 24/7 Network grew quickly to contain more than 70 member countries. Now, each of those member countries can send requests to ISPs in the United States.

These 24/7 Network letters are sent pursuant to 18 U.S.C. § 2703(f), which requires the preservation of evidence whenever a "governmental entity" requests that the provider do so pending forthcoming legal process. A "'governmental entity' means a department or agency of the United States or any State or

political subdivision thereof."[7] The United States government invokes Section 2703(f) because of the contemplated MLAT request.

What Do 24/7 Network Requests Look Like and What Do You Do?

Hundreds of these letters are issued by the Office of International Affairs of the United States Department of Justice every year.[8] Incoming[9] 24/7 Network requests come through the OIA. Therefore, an ISP will get a letter or similar written communication from the OIA requesting preservation of specific data. Those letters often request but do not require that the corresponding customer not be informed of the request. Since these letters are issued according to 18 U.S.C. § 2703(f), unless there is an accompanying order under 18 U.S.C. § 2703(b), there is no legal statutory or judicial reason to comply with a nondisclosure request except in the discretion of the served entity, pursuant to its customers' terms of service.

The 24/7 Network Versus the CLOUD Act

The CLOUD Act, signed into law in March 2018, raises the possibility of agreements between the U.S. and EU governments on law enforcement access to digital evidence.[10] On a separate, but similar path, is the EU's proposed "e-evidence" regulation, which would streamline law enforcement access to data among its 28 member states.[11] These two actions will greatly change the way that the 24/7 Network operates.[12]

Section 102(6) of the CLOUD Act authorizes the U.S. to enter into executive agreements with foreign governments to facilitate law enforcement access to cross-border data.[13] Countries with those executive agreements with the United States no longer need to go through the MLAT process to request communications content from U.S.-based providers.[14] Instead, they can directly request the data from U.S.-based providers. It is important to note that the CLOUD Act only applies to the data of foreigners located outside the United States.[15]

The CLOUD Act creates a new process for requests for U.S.-based data coming from agreeing countries. Those requests would come with the force of the new provisions in 18 U.S.C. § 2713: "Required preservation and disclosure of communications and records." Challenges to the requests would follow a motion to quash, the procedures for which are set forth in amendments to the already existing 18 U.S.C. § 2703.[16]

A motion to quash may be filed where the provider reasonably believes that the requested disclosure would create a material risk that the provider would violate the laws of a "qualifying foreign government." For the purposes of the CLOUD Act, a "qualifying foreign government" is one with which the United States has entered into an executive agreement, as defined by the new 18 U.S.C. § 2523.[17]

If the request targets a "United States Person," or a person located in the United States, the CLOUD Act request is invalid.[18] A "United States Person" is defined as "a citizen or national of the United States, an alien lawfully admitted for permanent residence, an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation that is incorporated in the United States." [19] In time, these CLOUD Act requests could eventually replace many 24/7 requests. However, they will never replace the 24/7 Network requests for data of "United States Persons," who cannot be the subject of CLOUD Act process from "foreign governments."

The CLOUD Act sets up a few potential problems for U.S. providers. First, as a veteran of cyber investigations, I know that the identity of a hacker is often not known until after the communications are examined. Because of this, United States providers are likely to receive many requests that purport to be under the CLOUD Act but will relate to "United States Persons." The CLOUD Act puts the burden of identifying the target on the provider, not the foreign government. It remains to be seen whether that burden is appropriate.

Even where the person or device is known, the new procedure will be unusual. The executive agreements, as defined by the new 18 U.S.C. § 2523, indicate that search warrants will be issued according to the law of the requesting nation.[20] Thus, a U.S. provider, in accordance with the CLOUD Act, will be served with a search warrant or other process that was issued according to that other country's laws. The process of certifying the adequacy of the agreeing country's laws, which is done by the attorney general, will not be subject to administrative or judicial review.[21]

Finally, the CLOUD Act does not discuss the method for serving these foreign data requests upon U.S. providers. Given the overlap between the two schemes, these requests could be communicated via the same 24/7 Network. However, the changes that will need to be made to accommodate search warrant requests, instead of mere preservation orders, are not yet clear.

The CLOUD Act Versus the European Commission's E-Evidence Rules

On April 17, 2018, the European Union unveiled their response to the CLOUD Act:[22] the "e-evidence" rules, including a regulation covering cross-border access to and preservation of electronic data held by service providers[23] and a law requiring service providers to appoint a legal representative within the EU if they do not have an office or other presence within the EU.[24] The e-evidence rules will allow a judicial authority in one EU nation "to obtain electronic evidence (such as emails, text, or messages in apps, as well as information to identify a perpetrator as a first step) directly from a service provider or its legal representative in another Member State." The provider will "be obliged to respond within 10 days, and within 6 hours in cases of emergency (compared to up to 120 days for the existing European Investigation Order or an average of 10 months for the MLAT process)."[25]

Services that would be subject to the e-evidence requirements include a broad range of communications services and apps as well as online services "for which the storage of data is a defining component," such as social media platforms, online marketplaces, and hosting services (cloud storage services). These rules, including the requirement of appointing an EU representative for service of process, will apply to all companies doing business on the internet that offer these services in the EU.[26] The EU's e-evidence rules are not yet in effect. The European Commission's proposal is currently being considered under the EU's legislative process. [27]

Logically, the "e-evidence" rules will eliminate many 24/7 Network requests from EU countries to the United States. After all, they can simply serve their newly mandatory representative with legal process in their home country. However, the e-evidence regulations will not apply to companies that do not offer their services in the EU. Also, there are dozens of countries outside of the EU that are still members of the 24/7 Network. Therefore, although the number of the 24/7 requests may change, they will remain at least for the non-EU and non-CLOUD Act countries.

Takeaways

While they bear the seal of the United States Department of Justice, these 24/7 Network letters are simply preservation requests. They are not backed by a grand jury subpoena or court order. No actual content would need to be handed over until, via an MLAT, a court order is obtained. That diplomatic process is long. Moreover, with the CLOUD Act as passed and the EU's "e-evidence" rules coming into effect soon, it may be difficult to determine what if anything you should do next. If you receive such a letter or request, whether 24/7, CLOUD or EU, you should first review it with counsel.

Chris Ott is a partner at Davis Wright Tremaine LLP and former senior counterintelligence and cyber counsel with the U.S. Department of Justice's National Security Division.

[1] NATO Cooperative Cyber Defence Centre of Excellence, "Group of Seven," https://ccdcoe.org/g7.html. The European Union has participated since 1981 as a "non-enumerated" member.[1] Russia joined in 1997 and the G7 became known as the G8 until 2014. When Russia annexed Crimea, it was expelled and the G7 designation returned.

[2] https://www.cnn.com/politics/live-news/trump-g7-2018/

[3] https://ccdcoe.org/g7.html

[4] Id.

[5] Id.

[6] Id.

[7] 18 U.S.C. § 2711(4).

[8] https://rm.coe.int/1680303ce2

[9] Outgoing 24/7 requests from the United States to other countries are handled by the Department of Justice's Computer Crimes and Intellectual Property Section.

[10] https://iapp.org/news/a/what-the-cloud-act-means-for-privacy-pros/. While the House Judiciary Committee and the Senate Judiciary Subcommittee on Terrorism and Crime have held hearings addressing the U.S.-U.K. agreement, the timeline for passing that agreement is still unclear.

[11] https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/e-evidence_en

[12] This paper does not focus on the United States government's ability to get at data stored in countries other than the United States, which is also covered by the CLOUD Act, passed in response to

the Microsoft case. https://www.nytimes.com/2018/04/17/us/politics/supreme-court-tosses-out-case-on-digital-data-abroad.html

[13] https://docs.house.gov/billsthisweek/20180319/BILLS-115SAHR1625-RCP115-66.pdf

[14] Those governments must commit to ensuring that U.S. law enforcement can directly request communications content from those countries' local providers—also enabling the United States to bypass the otherwise applicable mutual legal assistance process. Id.

[15] Id.

[16] 18 U.S.C. § 2703(h)(2) (proposed in https://docs.house.gov/billsthisweek/20180319/BILLS-115SAHR1625-RCP115-66.pdf).

[17] 18 U.S.C. § 2703(h)(1)(i) (proposed in https://docs.house.gov/billsthisweek/20180319/BILLS-115SAHR1625-RCP115-66.pdf).

[18] 18 U.S.C. § 2523 (b)(4) (A)-(C) (proposed in https://docs.house.gov/billsthisweek/20180319/BILLS-115SAHR1625-RCP115-66.pdf).

[19] 18 U.S.C. § 2523 (a)(2) (proposed in https://docs.house.gov/billsthisweek/20180319/BILLS-115SAHR1625-RCP115-66.pdf).

[20] 18 U.S.C. § 2523 (b)(4)(D) (proposed in https://docs.house.gov/billsthisweek/20180319/BILLS-115SAHR1625-RCP115-66.pdf).

[21] 18 U.S.C. § 2523 (c) (proposed in https://docs.house.gov/billsthisweek/20180319/BILLS-115SAHR1625-RCP115-66.pdf).

[22] https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/e-evidence_en

[23] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:225:FIN

[24] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:226:FIN

[25] https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/e-evidence_en

[26] http://europa.eu/rapid/press-release_MEMO-18-3345_en.htm

[27] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018PC0226&from=EN