New York Law Journal
Technology Today
WWW.NYLJ.COM
An ALM Publication
VOLUME 263—NO. 61
TUESDAY, MARCH 31, 2020

Data

How the CLOUD Act Is Likely To Trigger Legal Challenges

William Schwartz, Andrew Goldstein and Daniel Grooms

The CLOUD Act is about to stir up a legal storm. The Act was originally passed in March 2018 to ensure U.S. law enforcement officials could obtain information from U.S.-based communications providers even if that information is stored overseas. But the Act has another, more controversial provision: Under certain circumstances, it permits foreign law enforcement officials to serve production orders directly on U.S.-based providers and requires the providers to appear in court overseas if they want to challenge the orders. This possibility may soon be reality, as a novel data-sharing agreement under the Act between the United States and the United Kingdom takes effect this spring.

Until now, if foreign law enforcement officials wanted access to data held by U.S service providers, they had to go through Mutual Legal Assistance Treaties or "letters rogatory," which give U.S. providers the ability to challenge production orders in U.S. courts. But the U.S.-U.K. "Bilateral Data Access Agreement," which is the first such agreement under the CLOUD Act, cuts U.S. courts out of the process and allows U.K. law enforcement to serve production orders directly on U.S. providers. The Department of Justice is negotiating similar agreements with representatives from the European Union and Australia. While the stated purpose of these agreements is to speed up criminal investigations that have international dimensions, a side effect may be a burst of litigation—in both the U.S. and overseas—over issues of venue, privacy, disclosure, and due process.

The U.S. CLOUD Act And the U.K. COPOA

Before the CLOUD (Clarifying Lawful Overseas Use of Data) Act, when U.S. authorities served search warrants or subpoenas on U.S. communications providers, the law was unclear as to whether providers had to produce information that they stored overseas. Providers also faced uncertainty when *foreign* law enforcement authorities made requests for data, because the privacy provisions in the Stored Communications Act (SCA) contain an exception for U.S. law enforcement requests but not foreign requests. Foreign requests for data have become increasingly common due to the worldwide reach of U.S. providers.

The CLOUD Act clarifies that data needs to be produced regardless of where it is stored and that production to foreign law enforcement authorities does not violate the SCA. The Act also includes provisions

WILLIAM SCHWARTZ *serves as chair of Cooley's white collar defense & investigations group.* ANDREW GOLDSTEIN *and* DANIEL GROOMS *are partners in the group.*

intended to reduce the delay inherent in the MLAT and letter rogatory process, which often takes a year or more and requires substantial involvement by the Department of Justice. In particular, the CLOUD Act authorizes the U.S. government to enter into bilateral data-sharing agreements with countries that the Secretary of State and the Attorney General certify as having, among other things, "robust substantive and procedural protections for privacy and civil liberties." The agreements permit each country to issue production orders directly to communications-service providers located in the other country.

Last year the U.K. passed its own version of the CLOUD Act, the Crime (Overseas Production Orders) Act 2019 (COPOA). COPOA gives U.K. law enforcement agencies the means to apply for an English court order with extraterritorial effect that can compel production of stored electronic data directly from a company or person based in a foreign country with which the U.K. has a bilateral agreement for that purpose.

The Novel U.S.-U.K. Data Sharing Agreement

The U.S.-U.K. data sharing agreement, which was the first of its kind under the CLOUD Act, was announced on Oct. 3, 2019, and is scheduled to take effect this spring subject to no further action being taken by Congress and expiration of a ratification period in the U.K. In announcing the agreement, the Department of Justice claimed that it "will dramatically speed up investigations by removing legal barriers to timely and effective collection of electronic evidence." Focusing on cases involving terrorism, organized crime, and child exploitation, Attorney General Barr said, "Only by addressing the problem of timely access to electronic evidence of crime committed in one country that is stored in another, can we hope to keep pace with twenty-first century threats."

SHUTTERSTOCK

> Under certain circumstances, the CLOUD Act permits foreign law enforcement officials to serve production orders directly on U.S.-based providers and requires the providers to appear in court overseas if they want to challenge the orders.

Once the agreement takes effect, U.S. providers should expect to begin receiving orders directly from the U.K. Home Secretary on behalf of authorities in the U.K. such as the Police and Financial Conduct Authority. The orders will require the receiving company to respond directly to the relevant authority in the U.K. Under COPOA, the recipient of the order has, as a default, just seven days to produce the data covered by the order but can apply to a court in the U.K. to vary or set aside the order. Likewise, U.K.-based providers should expect to begin receiving orders directly from U.S. authorities.

The agreement contemplates that any challenge to an order will be brought in the courts of the country that issued the order, rather than in the country in which the recipient of the order is located. Legal challenges also are to be based on the domestic law of the issuing country—so that U.S. providers seeking to challenge a U.K. production order conceivably will have to bring the challenge in the U.K. under English, not U.S., law. In addition, challenges to production orders are to be made by communications providers themselves and not by their underlying customers whose data is at issue.

Potential Legal Challenges

Production orders issued under the Agreement are almost certain to trigger legal challenges on both sides of the Atlantic that will raise novel issues of domestic and international law.

Venue. Under the current MLAT process in the United States, a U.S.

federal district court reviews the foreign partner's request not only for compliance with the relevant MLAT, but also for compliance with U.S. statutory and constitutional law. The CLOUD Act and implementing agreement, in contrast, purport to circumvent the courts of the country in which the provider is based.

Judges in the United States may not be so quick to agree that they have no role, particularly in cases where a provider is raising constitutional challenges that English courts may not be as competent to adjudicate. This raises the possibility that early orders issued under the agreement could face parallel challenges in both U.S. and English courts, the ramifications of which could undermine both governments' goals of streamlining data-sharing in criminal investigations.

Privilege. Production orders under the agreement also are likely to raise difficult issues of privilege. Both the United States and the U.K. have laws protecting certain categories of privileged information from disclosure, and the text of COPOA itself provides a specific exception for confidential personal records and items subject to legal privilege. But the agreement does not specify how decisions about privilege or confidentiality should be made or who should make them. The issue is particularly tricky because production orders will be served on providers, not their customers, and the orders can be accompanied by non-disclosure provisions prohibiting their disclosure to the customers whose data is at issue. As a result, providers will have to navigate their own legal obligations under the agreement, which have the potential to clash with the privacy interests of their customers.

There also are important differences between U.S. and U.K. privilege rules, and the implementing agreement does not attempt to resolve them. For example, the protection of communications with in-house counsel is broader in the United States than under English law, as is the definition of what constitutes a "client" when dealing with a company's employees. U.S. law also provides broader protections for notes of interviews conducted in the course of internal investigations. Which rules apply, and who decides how to apply them, likely will need to be resolved through litigation.

> Production orders issued under the Agreement are almost certain to trigger legal challenges on both sides of the Atlantic that will raise novel issues of domestic and international law.

Constitutional and Domestic Law Challenges. Depending on the scope and language of a given production order, providers may be able to claim that the order does not comply with the implementing agreement because the request is overbroad or seeks evidence in an investigation not satisfying the criteria of the agreement. For example, providers may seek to challenge orders under COPOA on the basis that the order is not in the interest of justice considering the benefit likely to accrue from the data's use in the investigation or proceedings.

Providers also may argue that production orders violate fundamental or constitutional rights. For example, U.S. recipients of U.K. orders, particularly those with non-disclosure provisions, may wish to raise a constitutional challenge in U.S. courts based on the argument that the order, the CLOUD Act, or the implementing agreement violates the First Amendment or due process rights.

Privacy. U.K. recipients of U.S. orders may seek to challenge the agreement in their home courts on the ground that their obligations under the order are incompatible with the General Data Privacy Regulation (GDPR) prohibitions on the transfer of personal data outside the European Union. While the GDPR permits the transfer of personal data pursuant to an international agreement between public bodies, such as the agreement considered here, if the data sought is controlled by a UK company but held on a server outside of the UK (but within the European Union), given that the country hosting that data is not a signatory to the agreement, transfer of the data in compliance with a U.S. order may still be seen as a breach of the GDPR.

Reprinted with permission from the March 31, 2020 edition of the NEW YORK LAW JOURNAL © 2020 ALM Media Properties, LLC. All rights reserved. Further duplication without permission is prohibited. For information, contact 877-257-3382 or reprints@alm.com. # NYLJ-03302020-444632