AN A.S. PRATT PUBLICATION
JANUARY 2020
VOL. 6 • NO. 1

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 6 | NUMBER 1 | JANUARY 2020

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at 908-673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
Customer Service Web site ..... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (937) 247-0293

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [6] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [1] (LexisNexis A.S. Pratt)

An A.S. Pratt™ Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2020–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquiries and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 646.539.8300. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report,* LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

United Kingdom and United States Governments Sign First-Ever CLOUD Act Agreement

By Jonathan S. Kolodner, Nowell D. Bamberger, Rahul Mukhi, Alexis Collins, and Kal Blassberger*

The authors of this article discuss a recently signed first-ever executive agreement between the governments of the United Kingdom and United States governing cross-border data requests pursuant to the US Clarifying Lawful Overseas Use of Data Act ("CLOUD Act").

The governments of the United Kingdom and United States recently signed the first-ever executive agreement governing cross-border data requests (the "Agreement") pursuant to the US Clarifying Lawful Overseas Use of Data Act ("CLOUD Act"). As contemplated by the CLOUD Act, the Agreement provides a mechanism for the governments to access and share data stored abroad by electronic communications services providers ("CSP") in their respective countries in a timely manner.

The Agreement will enter into effect following a 180 day Congressional review period required by the CLOUD Act and a similar review by the UK Parliament.

BACKGROUND

The CLOUD Act was enacted in May 2018 to clarify that under a provision of the 1986 Stored Communications Act ("SCA") the U.S. government may use a warrant or subpoena to access not only communications stored in the United States but also those stored abroad by CSPs otherwise subject to jurisdiction in the United States. Included in the Act was a provision that allows the U.S. Attorney General to enter into executive agreements with foreign governments, when those foreign governments meet certain privacy and human rights requirements. As the Department of Justice ("DOJ") explained in its 2019 white paper, this new authority to enter into executive agreements with foreign governments is intended to lift legal barriers to gathering electronic evidence from global CSPs based in the United States and abroad, and will allow U.S. law enforcement agencies to require U.S. and foreign-based CSPs to disclose electronic

* Jonathan S. Kolodner (jkolodner@cgsh.com) is a partner at Cleary Gottlieb Steen & Hamilton LLP focusing on white-collar criminal enforcement and regulatory matters as well as complex commercial litigation. Nowell D. Bamberger (nbamberger@cgsh.com) is a partner at the firm focusing on cross-border complex contentious disputes, including litigation, investigations, and international arbitration. Rahul Mukhi (rmukhi@cgsh.com) is a partner at the firm handling criminal, securities, and other enforcement and regulatory matters as well as complex commercial litigation. Alexis Collins (alcollins@cgsh.com) is a partner at the firm concentrating on complex civil and antitrust litigation, criminal and regulatory enforcement matters, and cybersecurity. Kal Blassberger (kblassberger@cgsh.com) is an associate at the firm focusing on litigation.

data held abroad without making requests through judicial assistance procedures laid out in current mutual legal assistance treaties ("MLAT"), which can be a laborious process taking months to complete.

The CLOUD Act established certain minimum requirements that any order issued pursuant to future CLOUD Act agreements would need to incorporate, including, among others:

(i) That requests "be for the purpose of obtaining information relating to the prevention, detection, investigation, or prosecution of serious crime";

(ii) Identify specific accounts, addresses or persons;

(iii) Be based on "articulable and credible facts" related to the conduct under investigation; and

(iv) Be subject to review or oversight by a judge, magistrate or other independent authority.

Additionally, CLOUD Act agreements must contain measures to protect the data of U.S. persons that is collected incidentally to an order issued by a foreign government under such an agreement and the targeting of citizens and lawful residents of the United States by the foreign government.

THE CLOUD ACT AGREEMENT BETWEEN THE U.S. AND THE U.K.

As explained in Article 2 of the Agreement, the Agreement provides an efficient means for each of the countries "to obtain electronic data relating to the prevention, detection, investigation, or prosecution of Serious Crime," in a matter consistent with data privacy concerns and protective of the respective countries' citizens and lawful residents. "Serious Crime" is defined broadly as an "offense that is punishable by a maximum term of imprisonment of at least three years." While this definition excludes misdemeanors and minor felonies, it covers an otherwise wide range of crimes.

Under the Agreement, the country in which the data being sought is stored will have the right to object to and block an order issued pursuant to the Agreement seeking disclosure of that data. Absent any such objection, the CSP served with a request will be required to produce the data directly to the issuing authority. This differs from the way MLATs, which typically require the CSP only to produce the data to the central authority of the country in which the data is stored, operate.

Thus, the Agreement will allow the parties to access data through efficient and rapid means, regardless of where the data is stored.

Notably, however, the Agreement does not affect other existing legal methods. Consequently, U.S. law enforcement agencies will still be able to compel CSPs subject to U.S. jurisdiction to disclose data stored abroad by issuing appropriate process to the CSP and

enforcing it in federal district court, a mechanism that will often be the most expeditious method when seeking the disclosure of data from such CSPs.

Perhaps the most immediate practical impact of the Agreement is that U.S. law enforcement may now obtain communications from U.K. CSPs not subject to U.S. jurisdiction, and U.K. authorities may do the same with respect to U.S. CSPs. In addition, in the face of CSP's challenge to a warrant, U.S. courts conducting a comity analysis of a warrant issued by a U.S. law enforcement agency under the CLOUD Act's "totality of the circumstances" test are instructed to consider "the interests of the qualifying foreign government in preventing any prohibited disclosure."

Once the Agreement enters into effect, courts may find that the United Kingdom has no interest in preventing disclosure of the data being sought if it does not formally object to the warrant.

In addition to incorporating the requirements laid out above, the Agreement includes several other provisions of note that go beyond what is generically required by the CLOUD Act:

- Prior to the issuance of an order to a CSP, the order must be certified in writing by the issuing party's designated authority as lawful and in compliance with the Agreement. The designated authority is a governmental entity designated by the U.K. Secretary of State for the Home Department and the U.S. Attorney General.
- To the extent a CSP that receives an order pursuant to the Agreement has objections, the CSP may raise those objections to the issuing party's designated authority. In the event the objections are not resolved by the issuing party, the CSP may raise the objections to its own government's designated authority. If, after conferring with the issuing party's designated authority, the CSP's government determines that the order is not proper under the Agreement, the order will not be implemented.
- In the event an order issued subject to the Agreement seeks data of an individual who is located in a third country, the issuing party's designated authority must notify the country where the person is located, except insofar as the issuing party determines that such notification to the third country would be detrimental to its investigation or operational or national security, or threatens human rights.
- In addition to prohibiting the targeting of data with respect to citizens and lawful residents of the United States, as mandated by the CLOUD Act, the Agreement contains a reciprocal provision prohibiting the targeting of citizens and lawful residents of the United Kingdom by U.S. law enforcement agencies. However, law enforcement agencies in the United States may still seek to compel CSPs to disclose data with respect to citizens and lawful residents of the United Kingdom through the MLAT process.

CONCLUSION

As the first CLOUD Act agreement entered into by the United States with a foreign government, the Agreement will likely serve as a model for future agreements with other foreign governments. Accordingly, U.S.-based and foreign CSPs should familiarize themselves with the obligations and rights they will have when responding to an order issued under the Agreement even if they do not store data within the United Kingdom.

While the Agreement does not impose any new freestanding obligations on CSPs, it is important for CSPs to understand the new process contemplated by the Agreement for requiring disclosure of data stored abroad, particularly in light of the expedited timeline over which this process will now take place.

Importantly, the Agreement also has significant ramifications for non-CSPs. Companies that use email or cloud providers in the United States or the United Kingdom should assume that, once the Agreement enters into effect, U.S. and U.K. law enforcement agencies will be able to reach communications held by such providers through the processes contemplated by the SCA and the Agreement.