2018

Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0

Jennifer Daskal

Stanford Law Review Online

Volume 71 May 2018

ESSAY

Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0

Jennifer Daskal*

Introduction

On March 23, President Trump signed the CLOUD Act,[1] thereby mooting one of the most closely watched Supreme Court cases this term: the *Microsoft Ireland* case.[2] This essay examines these extraordinary and fast-moving developments, explaining how the Act resolves the Supreme Court case and addresses the complicated questions of jurisdiction over data in the cloud. The developments represent a classic case of international lawmaking via domestic regulation, as mediated by major multinational corporations that manage so much of the world's data.

I. The *Microsoft Ireland* Case

Argued in February 2018, the *Microsoft Ireland* case presented the Court with a novel question resulting from changing technology and the rise of the cloud. Does a U.S. warrant, issued pursuant to the 1986 Stored Communications Act (SCA),[3] reach emails and other communications content that are accessed and controlled by a U.S.-based company, but stored on a data server located outside the United States? The issue was one of statutory interpretation—requiring courts to divine the intent of an act written well before there was a globally interconnected internet. Several district courts concluded that the data, even if located extraterritorially, was within a U.S.-based provider's custody and control, and thus subject to the government's

* Associate Professor, American University Washington College of Law.

1. Clarifying Lawful Overseas Use of Data (CLOUD) Act, H.R. 1625, 115th Cong. div. V (2018) (enacted) (to be codified in scattered sections of 18 U.S.C.).
2. United States v. Microsoft Corp. (*Microsoft Ireland*), No. 17-2, slip op. at 3 (Apr. 17, 2018) (per curiam) (vacating and remanding judgment).
3. *See* Stored Communications Act, Pub. L. 99-508, tit. II, 100 Stat. 1848, 1860-68 (1986) (codified as amended at 18 U.S.C. §§ 2701-12).

warrant authority.[4] But the Second Circuit disagreed, and the government appealed to the Supreme Court.[5]

From the government's perspective, the Second Circuit's ruling was a significant security blow: It meant that any time sought-after data happened to be held outside of the United States, it had to request access via a foreign government—even if law enforcement were seeking data of a U.S. citizen regarding a U.S.-based crime, the data was controlled and accessible by a U.S.-based company, and the only foreign connection was that the data happened to be stored outside the United States' territorial boundaries.[6] In some cases, law enforcement didn't know where the data was located and thus where to direct the request; in other cases, the data might be held in a country that was unwilling to cooperate with the United States. Law enforcement also worried that nefarious actors would simply request data to be held extraterritorially to evade access.

Microsoft, by contrast, warned of a situation in which every country in the world would demand access to data of interest, simply because it had jurisdiction over the provider—or subsidiary thereof—that could access the data, irrespective of its location. This would, according to Microsoft, yield a free-for-all, international discord, and reduction in privacy rights for all.[7] And while Microsoft acknowledged that the underlying statute needed updating, it argued that warrants have territorial limitations, that its read of the statute was therefore the correct one, and that it was up to Congress, not the courts, to rewrite the law.[8]

At oral argument, several Justices seemed to agree that the issue belonged in the halls of Congress, not the Court. In the words of Justice Sotomayor, "[w]hy shouldn't we leave the status quo as it is and let Congress pass a bill in

4. *See, e.g.*, *In re* Search Warrant Issued to Google, Inc., 264 F. Supp. 3d 1268, 1279-80 (N.D. Ala. 2017); *In re* Search Warrant No. 16-960-M-1 to Google, 275 F. Supp. 3d 605, 619 (E.D. Pa. 2017), *aff'g* 232 F. Supp. 3d 708, 725 (E.D. Pa.); *In re* Warrant to Search a Certain E–Mail Account Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 466, 477 (S.D.N.Y. 2014), *rev'd*, 829 F.3d 197 (2d Cir. 2016).

5. United States v. Microsoft Corp., 138 S. Ct. 356 (2017) (mem.) (granting government's petition for certiorari).

6. *See* Brief for the United States at 41-45, *Microsoft Ireland*, No. 17-2, 2017 WL 6205806. Companies like Google—which network in a very different way than does Microsoft—pose a particular challenge for law enforcement. Google's data constantly moves across data centers distributed across the world, making it difficult if not impossible to employ the mutual legal assistance process as a means of accessing sought-after data. The result is that sought-after data may be beyond both U.S. *and* foreign law enforcement. *See id.* at 43-45; *see also* Paul M. Schwartz, *Legal Access to the Global Cloud*, 118 COLUM. L. REV. (forthcoming 2018) (manuscript at 8-13), https://perma.cc/Q4MT-KQQD (highlighting the legal implications of different network architectures).

7. Brief for Respondent at 30-32, 38-44, 58, *Microsoft Ireland*, No. 17-2, 2018 WL 447349.

8. *Id.* at 51-54.

this new age."[9] This position, however, first required a determination of what the status quo was—which is exactly what Microsoft and the U.S. government were fighting about.

The CLOUD Act allowed the court to avoid having to decide the issue—providing exactly the deus ex machina that the Court was hoping for. Specifically, the Act amends the SCA to address two distinct issues: the reach of U.S. warrant authority (the topic of the *Microsoft Ireland* case) and the converse problem faced by foreign governments seeking access to U.S.-held communications content. The following discussion addresses each.

II. The CLOUD Act and the *Microsoft Ireland* Fix

The CLOUD Act clarifies that service providers are required to disclose all data in their possession, custody, or control, pursuant to lawful process, regardless of the location of the data.[10] This requirement is consistent with the government's position in the *Microsoft Ireland* case. But the Act includes a critical addition—the enactment of a new statutory basis to quash based on comity grounds,[11] albeit in those situations in which the United States seeks the data of a foreigner located outside the United States, and the request generates a conflict with "qualifying" foreign governments. In such circumstances, courts are required to weigh a number of different factors—including the location and nationality of the person whose communications are being sought, the importance of the information to the United States' investigation, and the likelihood of timely and effective access to the evidence via alternative means.[12] Qualifying foreign governments are limited to those governments with which the United States has a data sharing agreement, as discussed below.[13] This is currently a null set, but one that is likely to grow.

The law also explicitly preserves, via a rule of construction, the availability of common law comity claims in those situations that do not involve a qualifying foreign government.[14] Such claims can be brought if and when the demand for data yields a conflict of laws; in response, a court will weigh the

9. Transcript of Oral Argument at 12, *Microsoft Ireland*, No. 17-2. Justice Ginsburg expressed a similar sentiment. *See id.* at 6 ("So wouldn't it be wiser just to say let's leave things as they are; if—if Congress wants to regulate in this brave new world, it should do it?").

10. H.R. 1625, 115th Cong. div. V, § 103(a) (2018) (enacted) (to be codified at 18 U.S.C. § 2713).

11. Such claims have a common law origin and are triggered by a conflict of laws, leading the court to take into account the respective interests of the United States and the foreign government in deciding whether to demand provider compliance. *See* Société Nationale Industrielle Aérospatiale v. U.S. Dist. Court for the S. District of Iowa, 482 U.S. 522, 555 (1987) (Blackmun, J., concurring in part and dissenting in part) ("[T]he threshold question in a comity analysis is whether there is in fact a true conflict between domestic and foreign law.").

12. CLOUD Act § 103(b) (to be codified at 18 U.S.C. § 2703(h)).

13. *Id.*

14. *See id.* § 103(c).

competing U.S. and foreign government interests in deciding whether to force compliance with the warrant.[15] Notably, no comity claim has ever been invoked in connection with an SCA warrant—in part because no provider has ever alleged that compliance with such a warrant would generate a conflict of laws. In fact, even in the *Microsoft Ireland* case, there was never any claim of legal conflict.

The European Union's (EU's) General Data Protection Regulation (GDPR),[16] which is set to go into effect in May 2018, may change this, yielding new claims of conflict. The GDPR sets a number of limitations on when EU-held data may be transferred out of the EU, including in response to court orders issued by non-EU countries. Article 48 of the GDPR specifies that such orders may only be recognized if based on an international agreement, such as a mutual legal assistance treaty, but "without prejudice to other grounds for transfer."[17] Given that there is no such international agreement that would authorize a provider to transfer EU-held data in response to a U.S.-issued warrant, an alternative basis is needed for transfer to be permitted under EU law.

There are two likely possibilities, both laid out in Article 49 of the Directive. First, transfers are permissible if "necessary for important reasons of public interest"[18]—a standard that would seem to encompass, at least in certain circumstances, the public interest in investigating and prosecuting serious crime. Second, transfers are permissible if necessary for "compelling legitimate interests" of the controller not overridden by the interests of the data subject, not repetitive, and concerning only a limited number of data subjects[19]—a provision that could justify transfers if providers would otherwise be subject to a U.S.-issued contempt order or other legal sanction.

That said, whether and to what extent these exceptions would apply is open to ongoing discussion, debate, and speculation. Even those European officials who agree that Article 49 would allow for transfers in certain circumstances warn that the grounds for transfer "are to be interpreted strictly"[20] —thus suggesting a case-by-case exploration of whether the transfer is permitted. And absent an applicable exception, a company that transfers data in response to an SCA warrant will be violating EU law.

---

15. *See* Brief for Amici Curiae E-Discovery Institute et al., in Support of Neither Party at 7-16, *Microsoft Ireland*, No. 17-2 (Apr. 17, 2018) (per curiam), 2017 WL 6492198 [hereinafter E-Discovery Brief].
16. Council Regulation 2016/679, 2016 O.J. (L 119) [hereinafter GDPR].
17. *Id.* art. 48 (discussing transfers not authorized by EU law).
18. *Id.* art. 49, § 1(d).
19. *Id.* art. 49, § 1; *see also* Brief of the European Commission on Behalf of the European Union as *Amicus Curiae* in Support of Neither Party at 12-16, *Microsoft Ireland*, No. 17-2, 2017 WL 6383224 [hereinafter EC Brief].
20. EC Brief, *supra* note 19, at 16.

Ideally, emerging conflicts will push the EU and United States to negotiate new international agreements to explicitly permit transfers in legitimate cases and to detail the procedural and substantive standards that apply. In the interim, both the substantive issues (do warrants for EU-held data conflict with EU law?) and more basic questions (can a provider bring such a challenge in response to the issuance of the warrant or is there a requirement to wait until contempt proceedings have been initiated?) are likely to be the source of future litigation.[21]

III. Foreign Government Access to U.S.-Held Content

The second part of the CLOUD Act addresses the *converse* problem of foreign governments seeking access to communications content that is U.S. held. This issue arises because the SCA prohibits U.S.-based providers from disclosing communications content to foreign governments, even if they are investigating their own citizens in connection with a local crime. These blocking provisions have been an increasing source of frustration for foreign governments, as more and more of the evidence sought in foreign criminal investigations is located in the hands of U.S.-based providers. In order to access such U.S.-held communications content, foreign governments must make a diplomatic request for the data, employing the mutual legal assistance treaty (MLAT) system. This is a cumbersome and often time-consuming process; according to the 2013 Report and Recommendations of the President's Review Group on Intelligence and Communications Technology, delays have averaged almost a year for such requests.[22]

The CLOUD Act seeks to address this problem. It provides a mechanism for select foreign governments to bypass the MLAT system in their investigation of serious crime and directly request sought-after communications from U.S.-based providers, pursuant to an executive agreement entered into between the foreign government and the United States, and pursuant to a long list of baseline substantive and procedural requirements. Foreign governments are only eligible to enter into these agreements if the Attorney General, in conjunction with the Secretary of State, certifies in writing, and with an accompanying explanation, that the foreign government "affords robust substantive and procedural protections for privacy and civil

21. *See* CLOUD Act, H.R. 1625, 115th Cong. div. V, § 103(b) (2018) (enacted) (to be codified at 18 U.S.C. § 2703(h)); *see also* E-Discovery Brief, *supra* note 15, at 17-21 (warning that the courts too often treat comity "as a formality" and do not adequately take into account the interests of foreign governments).

22. *See* RICHARD A. CLARKE ET AL., LIBERTY AND SECURITY IN A CHANGING WORLD: REPORT AND RECOMMENDATIONS OF THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES 227 (2013) (noting that it takes an average of about ten months to process MLAT requests).

liberties" with respect to relevant data collection activities.[23] The foreign government must agree to reciprocal rights of access by the United States to foreign government-held data; must adopt appropriate minimization procedures with respect to the acquisition, retention, and dissemination of U.S. person data; and is prohibited from using the agreement to require that providers be capable of decrypting otherwise encrypted data.[24] Agreements cannot go into effect until Congress has six months to review them; the legislation specifies expedited procedures for Congress to enter into a joint resolution of disapproval.[25]

Each individual request issued by a foreign government also must meet specified baseline standards and requirements. Among other requirements, the requests need to be particularized—targeting a *specific* person, account, address, personal device, or other identifier; be based on "articulable and credible facts"; be subject to "review or oversight by a court, judge, magistrate, or other independent authority"; and not be used to infringe speech.[26] Live intercept orders must be for a "fixed, limited duration," "not last longer than is reasonably necessary to accomplish the approved purposes," and "be issued only if the same information could not reasonably be obtained by another less intrusive method."[27]A particularly novel development requires the foreign government to agree to "periodic review of compliance . . . to be conducted by the United States Government."[28]

Importantly, the agreements only authorize the foreign government to access data of foreigners located outside the United States. To access the data of U.S. citizens, legal permanent residents, and others located within the United States, the foreign government must continue to employ the MLAT process. This difference respects the commonsense notion, grounded in principles of democratic accountability, that governments have an interest in setting standards and rules regarding access to their own citizens' and residents' data; they don't have an equivalent interest in setting the rules with respect to foreign governments accessing foreigners' data.

The United Kingdom has reportedly been in discussion with the United States about a possible agreement for years and is therefore likely to be the first government to enter into such an agreement, although the text of any such agreement has not yet been finalized or released to the public.[29] The question

23. CLOUD Act § 105(a) (to be codified at 18 U.S.C. § 2523(b)).
24. *Id.*
25. *Id.* (to be codified at 18 U.S.C. § 2523(d)).
26. *Id.* (to be codified at 18 U.S.C. § 2523(b)).
27. *Id.*
28. *Id.*
29. *See Data Stored Abroad: Ensuring Lawful Access and Privacy Protection in the Digital Era: Hearing Before the H. Comm. on the Judiciary*, 115th Cong. 3 (2017) (statement of Paddy McGuiness, Deputy National Security Adviser, United Kingdom).

of who comes next looms large. Here, too, there are a range of interesting and novel issues to work out, including the possibility of regional agreements, perhaps with a mechanism by which all requests are managed by a centralized authority that can ensure compliance with the statutory requirements.[30] Each individual country would still need to meet the requisite, overarching human rights standards, but the use of a centralized requesting body like this could facilitate accountability and review.[31]

IV. New Form of International Lawmaking

These provisions regarding foreign government access to U.S.-held data represent a new form of international lawmaking via domestic regulation, mediated by the major multinational companies that manage so much of the world's data. If successful, the substantive and procedural privacy standards that are preconditions for entering into bilateral agreements will be adopted by a growing list of foreign governments, thereby *raising* the privacy standards that apply. In fact, it appears that this increase has already started. The U.K. government supported a new judicial review provision with respect to compelled disclosure orders for data in part because it anticipated that provision being a precondition to be eligible for such an agreement with the United States. Other countries will ideally be motivated to raise privacy protections as well.[32] Provisions requiring auditing and compliance reviews provide an additional mechanism for the United States to insist on application of its domestic-imposed rules.

The CLOUD Act thus represents an effort by the United States to set international standards, but via domestic regulation rather than a global meeting of governments, or even a subset of such governments, working out new standards and rules.

The GDPR, discussed above, is another such example. The applicable privacy standards and transfer restrictions of the GDPR apply to *any* company directing business at the EU market or otherwise monitoring EU data subjects.[33] The GDPR thus applies its obligations even to companies that are not physically located within the EU. Even small companies that don't currently serve or direct their business to EU customers are being incentivized to do the kind of data mapping required by the EU; this preserves their potential marketability to larger companies that do, in fact, serve the EU market.

---

30. See Jennifer Daskal & Peter Swire, *Suggestions for Implementing the CLOUD ACT*, LAWFARE (April 30, 2018, 9 AM), https://perma.cc/UVP8-6M3A.
31. *See* Peter Swire & Deven Desai, *A "Qualified SPOC" Approach for India and Mutual Legal Assistance*, LAWFARE (March 2, 2017 12:14 PM), https://perma.cc/8ZFN-SLQE.
32. *See* Jennifer Daskal & Peter Swire, *Why the CLOUD Act is Good for Privacy and Human Rights*, JUST SECURITY (Mar. 14, 2018), https://perma.cc/7564-BEL3.
33. GDPR, *supra* note 16, art. 3, § 2.

This kind of international lawmaking via local regulation is not new, of course. Anu Bradford has aptly coined this the Brussels effect, based largely on the range of health and safety standards being exported by the EU.[34] But the rise of major multinational corporations that manage so much of the world's data—in ways that have profound implications for privacy, security, speech, and associational rights—takes this kind of international rulemaking into a new arena. In the best-case scenario, such efforts will lead to norm convergence and the adoption of standards, as mediated by these large multinational companies, that protect both privacy and security. In the less ideal scenario, countries may be increasingly incentivized to pursue data localization and market segmentation as a means of reasserting control.[35]

34. *See* Anu Bradford, *The Brussels Effect*, 107 NW. U. L. REV. 1, 5-10, 19-35 (2012); *see also* Austen L. Parrish, *Reclaiming International Law from Extraterritoriality*, 93 MINN. L. REV. 815, 832-56 (2009).

35. For a further, in-depth discussion of these issues of extraterritorial regulation via local regulation, see Jennifer Daskal, *Borders and Bits*, 71 VAND. L. REV. 179, 180-86, 232-39 (2018). *See also* Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 GEO. L. J. 115, 165-68 (2017) (highlighting the emergence of new kinds of governmental networks to address cross-border conflicts over data and the underlying privacy and related norms that apply).