Unpacking the CLOUD Act

Jennifer Daskal

eucrim
European Law Forum: Prevention • Investigation • Prosecution

Article

ABSTRACT

This article seeks to demystify the recently enacted Clarifying Lawful Overseas Use of Data (CLOUD) Act, enacted in March 2018 by the U.S. government in an effort to address challenges faced by law enforcement in accessing data located across borders. It explains the two parts of the act, dealing with: (i) U.S. access to data located outside the United States; and (ii) foreign government access to data held by U.S. companies within the United States. As the article highlights, the CLOUD Act offers a model for both responding to law enforcement needs and setting – and raising – baseline privacy protections. In that regard, it is a step in the right direction, although there is much more work to be done.

AUTHOR

Jennifer Daskal

Associate Professor
American University Washington

CITATION SUGGESTION

J. Daskal, "Unpacking the CLOUD Act", 2018, Vol. 13(4), eucrim, pp220–225. DOI: https://doi.org/10.30709/eucrim-2018-022

Published in
2018, Vol. 13(4) eucrim pp 220 – 225
ISSN: 1862-6947
https://eucrim.eu

I. Introduction

In March 2018, the United States enacted the Clarifying Lawful Overseas Use of Data (CLOUD) Act, mooting a pending Supreme Court case, detailing the reach of U.S. law enforcement authority over extraterritorially located data, and setting out a mechanism for foreign governments to gain expedited access to U.S.-held data in specified circumstances.[1]

The Act has generated controversy both within and outside the United States. Critics described it as having been "rushed" through Congress at the expense of privacy and civil liberties.[2] Others decried the "expansion of US enforcement power."[3] But, as this article explains, the rhetoric does not match the reality.

That said, there remain key, unresolved issues that need to be worked out, both by U.S. courts and in coordination with foreign partners in Europe and elsewhere; how these issues are resolved will go a long way towards determining the effectiveness of the Act as well as its effect on both privacy and security.

It is true that the legislation was tacked onto an omnibus spending bill at the 11th hour. But it was not the surprise that some have suggested. On the contrary, key elements had been the subject of hearings in both the House and Senate judiciary committees and in multiple other open, informal congressional briefings.[4] What ultimately became Part II of the Act was something that had been actively pursued by the Obama administration and ultimately also supported by the Trump administration. Tech companies, law enforcement officials, academic experts, and members of civil society were involved in a multi-year discussion of the issues; many representatives actively lobbied members of Congress both for and against key provisions.[5] An earlier version of the CLOUD Act had been previously proposed as a stand-alone bill.[6]

Moreover, whereas much of civil society argued – both before and after – the Act's passage that the baseline protections included in the second part of the Act do not sufficiently protect privacy and civil liberties, those baseline requirements are a *floor*—not a ceiling. Specifically, the Act authorizes the executive branch of the United States to enter into agreements with foreign governments, pursuant to which foreign governments can gain expedited access to U.S.-held data. In so doing, it sets out the *minimal* requirements that each and every agreement must meet. The envisioned agreements also impose a number of use-based limitations, mandating, for example, the secure storage of any disclosed data, deletion or segregation of non-relevant information, and limits on when the data can be shared. They also require that foreign partners agree to periodic reviews to ensure that the requirements are met.

In many areas, even these minimal requirements are more robust than what would be required if governments were able to compel the production of sought-after communications content pursuant to their existing domestic rules; this provides an incentive for governments to raise standards to meet the minimal requirements – an incentive that will ultimately enhance privacy protections above and beyond the status quo.

In addition, the first part of the Act, which clarifies the reach of US law enforcement over extraterritorially held data, is neither the kind of sea change nor the enforcement grab that some have suggested.[7] Prior to December 2013, when Microsoft first challenged a U.S.-issued warrant based on the fact that the sought-after data was located outside the territorial borders of the United States, providers regularly responded to U.S.-issued disclosure orders without regard to the location of the data being sought. A company like Google operates what has been called by a "data shard" model,[8] referring to the fact which the data of even a single account is sometimes broken up and moved from place to place, in many cases across international borders, for reasons of performance and efficiency. · As of 2017, Google did not have a mechanism in place

to ascertain where all of its data was located at any given point in time.[9] It only developed the tools to ascertain data location when, as a result of court rulings, it was required to do so.

As with all legislation, the CLOUD Act was the product of negotiated compromise; it is, as a result, inherently imperfect. Among other flaws, it does not contemplate the possibility of multilateral agreements, thereby leaving unresolved key questions about the possibility and contours of a potential US-EU agreement;[10] adopts a new conflict-of-law provision yet only applies it in very limited circumstances; fails to tackle the critically important issue of user notice; and neglects to provide explicit protection for companies that seek to provide transparency over foreign government requests for data, But it also reflects a much-needed attempt to respond to the changing needs of law enforcement, establish new mechanisms to address these needs, and lay out minimal substantive and procedural standards to govern law enforcement in the process. In so doing, it responds to three emerging realities:

- The increased digitalization of information;
- The power of third-party private companies that manage and control so much of that data;
- The increased internationalization of investigations, with either the data of interest or the provider that controls that data located across an international border.

As just one measure of these developments, a recent European Commission report found that law enforcement sought data held by extraterritorially-located service providers in over 55% of EU law enforcement investigations.[11] In many cases, that jurisdiction is the United States – a reality that the CLOUD Act tries, in part, to deal with. The first section of this article seeks to move past the rhetoric and demystify the CLOUD Act by explaining and analysing its two key parts. The second section highlights some of the key issues left to be resolved.

II. Unpacking the CLOUD Act

The CLOUD Act contains two key parts. Part I clarifies the reach of US law enforcement to access data held extraterritorially by US-based providers. Part II authorizes the executive to enter into agreements with foreign governments, pursuant to which foreign governments can bypass the otherwise applicable mutual legal assistance requirements in specified circumstances and according to baseline substantive and procedural requirements. The next two subsections provide details on each of these two parts.

1. The reach of US law enforcement

Just one month before the CLOUD Act's enactment, the Supreme Court heard oral arguments in what is often referred to as the *Microsoft Ireland* case. The case dates back to December 2013, when Microsoft was served with a warrant for emails, pursuant to the Stored Communications Act (SCA), as part of a drug-related criminal investigation. The sought-after emails were stored in Dublin, Ireland, and Microsoft refused to comply with the warrant as a result. According to Microsoft, warrants issued pursuant to the SCA are territorially limited and thus only could compel the production of data that was stored within the territorial jurisdiction of the United States.

The U.S. government acknowledged that the warrants authorized by the SCA do not have extraterritorial effect. But it emphasized that Microsoft was a U.S.-based company that could access and control the data from within the United States. According to the U.S. government, the fact that the particular 0s and 1s were

located outside the United States did not matter. What mattered was the location of access and disclosure – all within the territory of the United States.

In sum, both parties agreed that warrants issued under the SCA are territorially limited. But they strongly disagreed as to whether or a warrant issued on a U.S-located company for data located outside the United States was a territorial or extraterritorial exercise of the warrant authority. To resolve this dispute, the justices needed to identify the intent behind, and thus focus of, the SCA – a 30-plus-year-old statute that did not directly address the question posed. At the oral argument, several justices suggested that this was an issue better dealt with by Congress than the courts.[12]

And in fact, Congress stepped in just one month later, passed the CLOUD Act and answered the key unresolved question, and thereby mooted the Supreme Court case.

Consistent with the government's position in the case, the CLOUD Act specifies that providers are, in response to lawful process, required to disclose responsive communications content within their possession, custody, or control, regardless of the location of that data.[13] But Congress also recognized the risk of conflicts with foreign law, particularly in situations in which the request seeks extraterritorially held data of a foreign national. It thus created a new statutory basis for providers to move to quash based on a conflict with foreign law, albeit only in those limited circumstances in which the conflict is with a "qualifying foreign government" and the United States seeks the data of a non-U.S. person located outside the United States.[14] To become a qualifying foreign government, the government must have entered into an executive agreement with the United States as authorized pursuant to Part II of the Act. To date, there are *zero* such qualifying governments although that is likely to change over time as will be described below.[15]

Congress further noted the possibility that separate comity claims could be considered under "common law" standards in those circumstance in which statutory provision does not apply.[16] This would arise if, for example, a provider alleged that a compelled disclosure order conflicted with foreign law prohibiting such disclosure. Courts would then be in a position of weighing the relevant equities in deciding whether to continue to compel disclosure of the sought-after data. Notably, these kinds of claims could be made before and after the CLOUD Act's enactment; the CLOUD Act merely notes a continuation of the status quo. That said, Congress's explicit recognition of the need for courts to address legal conflicts gives credibility to such claims if and when they do arise.

As far as is known, no such claims of conflict in response to the issuance of U.S. warrants have yet been raised.[17] Even in the *Microsoft Ireland* case, neither Microsoft nor Ireland asserted a direct conflict of law. In its amicus brief to the Supreme Court, Ireland emphasized that it was willing and ready to respond to a mutual legal assistance request for the sought-after data. But it never actually asserted that Microsoft would violate Irish law if it were compelled to disclose the data.[18] That said, such conflicts are likely to emerge over time, given, in particular, transfer restrictions included in the EU's General Data Protection Regulation and as discussed below.[19]

2. Foreign law enforcement to U.S.-held data

Part II of the CLOUD Act responds to the converse problem foreign governments face with respect to their ability to access communications content held by U.S. service providers. The same statute at issue in *Microsoft Ireland*, namely the SCA, blocks US-based providers from disclosing communications content to foreign law enforcement. Instead, foreign law enforcement authorities are required to make a government-to-government mutual legal assistance request for such data, even if they are seeking the data of one of their own citizens or residents in connection with a local crime. This is a time-consuming process involving a

Department of Justice review of the request, a U.S. attorney's office going to court to obtain a warrant on behalf of the foreign government, and a subsequent review by the Department of Justice before the data is ultimately disclosed.[20] A 2013 report found that it took an average of ten months for the U.S. government to respond, even in those situations in which it agreed to turn over the data.[21]

Foreign governments are increasingly frustrated by this reality, given, in particular, the fact that US-based companies control such a significant quantity of the world's data and given the ways in which these requirements thwart the efforts to swiftly and efficiently investigate crime. Paddy McGuiness, the UK's former Deputy National Security Advisor, twice testified before the U.S. Congress about the ways in which the provisions blocking direct disclosures to foreign law enforcement were hampering the U.K.'s ability to investigate and prevent crime.[22]

To address these concerns, Congress authorized the executive branch to enter into agreements with foreign governments, pursuant to which the partner government could directly request communications content from U.S.-based providers, subject to specified requirements, without having to employ the mutual legal assistance process. In order to be eligible, the foreign government must first be certified by the Attorney General, in conjunction with the Secretary of State, as "afford[ing] robust substantive and procedural protections for privacy and civil liberties."[23] Each individual request must also meet specified requirements, including those that the requests be particularized, in compliance with the foreign government's domestic law, based on "articulable and credible facts" and subject to review or oversight by a court, judge, or magistrate or other independent authority of the requesting foreign government.[24] Requests must be limited to "serious crimes."[25]

Congress also anticipated the possibility that, pursuant to such agreements, foreign governments could seek live intercepts – and not just stored communications. For live intercepts, the legislation includes the additional requirements that the orders be time-limited, lasting no longer than is needed to accomplish the approved objectives, and subject to a finding that the same information "could not reasonably be obtained by another less intrusive method."[26]

The agreements also include a number of requirements as to use of collected data. The data must be stored on a "secure system" accessible only to those "trained in applicable procedures."[27] The foreign government is required to segregate, seal, or delete non-relevant information.[28] In addition, the foreign government must agree to periodic reviews by the United States government to ensure that the provisions of the executive agreement are being followed.[29] Whereas some such use-based limitations and accountability provisions were already included in the EU-US Umbrella Agreement, which covers law enforcement sharing across the Atlantic, these provisions include additional specifics that will help to protect the security and privacy of shared data.[30] Furthermore, for countries outside the EU that are not subject to the Umbrella Agreement, they represent a significant increase in protection compared to the status quo under the current mutual legal assistance process, where the U.S. government has minimal say as to how data is handled once it is provided to a foreign government.

Notably, the agreements also only permit foreign government direct access to the data of non-U.S. persons located outside the United States. Thus, even with an executive agreement in place, partner governments cannot directly compel the production of a U.S. person's (defined to include U.S. citizens and legal permanent residents)[31] communications content or the communications content of non-U.S. citizens physically located in the United States; these requests still need to go through the mutual legal assistance system.[32] In other words, partner foreign governments can directly access foreigners' data and hence set the rules, albeit with a number of baseline requirements in place, concerning access to that data. But if they want

access to U.S. citizen and resident data, they still need to get U.S. court approval based on the U.S. standard of probable cause.

Finally, the foreign government must provide "reciprocal rights of data access." This means that the foreign government must permit its own locally based providers to respond directly to U.S. requests for data if and when the United States is seeking the data of a non-national of the partner government, has issued valid legal process to the provider, and has jurisdiction to compel such production.[33]

III. Open Questions

The CLOUD Act is still new, leaving key questions as to implementation and interpretation to be worked out. Despite the warnings that Part I would lead to widespread conflicts of law, no such claims have yet been raised, although some may emerge in the near future. Of particular relevance, the EU's newly implemented General Data Protection Regulation includes key limitations on when EU-held data can be transferred out of the EU.[34] Some have argued that, in the absence of a new international agreement explicitly providing for transfers in these situations, no currently applicable exception would permit transfers of EU residents' data to the United States outside of the mutual legal assistance process, even in response to a validly U.S.-issued warrant.[35] The European Commission's amicus brief to the Supreme Court was non-committal on this point.[36] In the absence of an explicit EU-US agreement providing the basis for such transfers, conflicts may very well occur, with litigation to ensue.[37]

Meanwhile, no executive agreements have yet been entered into (and hence there are no "qualifying countries" for purposes of Part I of the CLOUD Act), although there are expectations that a U.S.-UK agreement will be forthcoming. Either a U.S.-EU framework agreement or agreements with specific EU countries may be next. These initial agreements are likely to become a model for those that follow.

Importantly, and as noted in the Introduction of this article, the statutorily specified requirements for executive agreements merely set a floor not a ceiling. Additional protections can, and in some cases should, be added to any agreements that are ultimately adopted. Among the key additional provisions to be included:[38]

- An agreed-upon mechanism for providers to initiate a U.S.-government review mechanism if and when they have concerns about a foreign government request;
- Protections for providers that produce transparency reports with details about foreign government requests for data;
- Clear rules on whether, when, and in what circumstances notification to the target of the collection is required and when and for what reasons it can be delayed.

Use-based requirements also provide an opportunity to incorporate protections in new and innovative ways. The required limitations on access, dissemination, and retention should be robustly implemented and followed. Periodic reviews should be regular and meaningful to ensure effective prevention and rapid correction of any errors or abuse.

A range of other details still needs to be worked out, including the scope of free speech protections and the set of "serious crimes" to be covered by the agreements.

Each and every agreement also will need to address issues of scope. The CLOUD Act, for example, authorizes agreements that cover both stored communications and live intercepts. But there is no requirement that

agreements do, in fact, encompass both. In fact, there is no basis in U.S. law to issue a wiretap order with extraterritorial reach.[39] It is thus possible to design agreements that allow for direct production of stored communications but do not include wiretaps.

In order to facilitate both compliance and oversight, partner countries might consider channelling all applicable cross-border requests through specified points of contact to ensure that specified protections are met. This is also something that the United States might require in certain circumstances. It also would help facilitate the periodic reviews and accountability that the agreements require. Each of these determinations can and should be worked out as part of an ongoing dialogue with the United States and key stakeholders from both industry and civil society. The considerations outlined here are just some of many.

IV. Conclusion

The CLOUD Act represents the opening salvo in a much-needed dialogue about the substantive and procedural rules governing law enforcement access to digital evidence and the shifting relationship between territorial boundaries and evidentiary needs. It is just one of many initiatives being pursued because of shifting trends in the ways key evidence is managed and stored. The European Union's draft e-Evidence proposals, unveiled in April 2018,[40] represent Europe's contribution to this discussion and bear remarkable similarities to the CLOUD Act. Akin to Part II of the CLOUD Act, the draft E-Evidence Regulation provides a mechanism for law enforcement in an investigating country to bypass the mutual legal assistance process and issue a disclosure order directly to a private company that holds evidence of interest, even if that private company is located outside the investigating country's territorial jurisdiction.

Other unilateral initiatives abound. As a result of recent legislative changes, the UK now authorizes the issuance of extraterritorial warrants. Australia recently enacted legislation that would authorize the issuance of technical assistance orders on extraterritorially-located providers that have one or more end users in Australia.[41] In specific court cases, Belgian authorities have maintained their authority to compel the production of data held by foreign-based providers offering services within Belgium, even if they are not located there.[42]

These initiatives seek to respond to the increasing digitalization of information, the role of third-party providers in controlling this information, and the fact that providers and data of interest are increasingly held across borders. These shifts provide opportunities as much as they create challenges. The U.S. CLOUD Act is an important contribution to these efforts – one that can and should be built on via the construction of robust bilateral agreements that protect and elevate privacy and civil liberties while at the same time facilitating lawful access in ways that help protect and promote security.

---

1. Clarifying Lawful Overseas Use of Data (CLOUD) Act, Pub. L. No. 115-141, 132 Stat. 348 (2018).↩
2. See N. Nielsen, "Rushed US Cloud Act Triggers EU Backlash", *euobserver* (26 March 2018), <https://euobserver.com/justice/141446> accessed 12 December 2018; D. Heide et al., "European Criticism of New US Cloud Act Mounts", *Handelsblatt Global* (24 April 2018), <https://global.handelsblatt.com/politics/with-new-us-law-how-safe-is-online-data-in-europe-914956> accessed 12 December 2018.↩
3. S. Richmond, "US CLOUD Act Raises New Data Privacy Issues", *Verne Global* (12 July 2018), <https://verneglobal.com/blog/us-cloud-act-raises-new-data-privacy-issues> accessed 12 December 2018.↩
4. See, e.g., *Subcommittee on Crime and* Terrorism, "Law Enforcement Access to Data Stored Across Borders: Facilitating Cooperation and Protecting Rights", Hearing Before the S. Judiciary, *115th Cong. (2017),* <https://www.judiciary.senate.gov/meetings/law-enforcement-access-to-data-stored-across-borders-facilitating-cooperation-and-protecting-rights> accessed 12 December 2018; *Data Stored Abroad: Ensuring Lawful Access and Privacy Protection in the Digital Era*: *Hearing Before the H. Comm. on the Judiciary*, 115th Cong. (2017), <https://judiciary.house.gov/legislation/hearings/data-stored-abroad-ensuring-lawful-access-and-privacy-protection-digital-era> accessed 12 January 2019; *International Conflicts of Law Concerning Cross Border Data Flow and Law Enforcement Requests: Hearing Before the H. Comm. on the Judiciary*, 114th Cong. (2016).↩
5. See, e.g., J. Daskal and A. K. Woods, "Cross-Border Requests: A Proposed Framework", *Just Security* (24 November 2015), <https://www.justsecurity.org/27857/cross-border-data-requests-proposed-framework/> accessed 12 December 2018 (proposing in 2015 a framework very similar to that enacted in 2018 as part of the CLOUD Act).↩
6. See S.2383 (115th Cong.); H.R. 4943 (115th Cong.).↩

7. See E. Wenger, "Does the CLOUD Act Really Grant DOJ Sweeping New Powers?", *Cross-Border Data Forum* (27 August 2018), <https://www.cross-borderdataforum.org/does-the-cloud-act-really-grant-doj-sweeping-new-powers/> accessed 12 December 2018 (making a similar point).↩
8. P. M. Schwartz, "*Legal Access to the Global Cloud*", (2018) 118 *Colum. L. Rev*., 1681, 1695 .↩
9. *In re* Search Warrant No. 16-960-M-01 to Google, 232 F. Supp. 3d 708, 723 (E.D. Pa. 2017).↩
10. J. Daskal and P. Swire, "A Possible EU-US Agreement on Law Enforcement Access to Data?", *Lawfare* (21 May 2018), <https://www.lawfareblog.com/possible-eu-us-agreement-law-enforcement-access-data> accessed 12 December 2018.↩
11. European Commission, "Commission Staff Working Document Impact Assessment, Accompanying the Document, Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters and Proposal for a Directive of the European Parliament and of the Council Laying Down Harmonised Rules on the Appointment of Legal Representatives for the Purpose of Gathering Evidence in Criminal Proceedings", SWD(2018) 118 final, p. 14.↩
12. See J. Ginsburg, Transcript of Oral Argument, *United States v. Microsoft Corp.*, 138 S. Ct. 1186 (2018) (No 17-2), <https://www.supremecourt.gov/oral_arguments/argument_transcripts/2017/17-2_j4ek.pdf> accessed 12 December 2018, p. 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?"; J. Sotomayor, *ibid.,* p. 12: ("Why shouldn't we leave the status quo as it is and let Congress pass a bill in this new age"; J. Alito, J., *ibid.,* p. 36: "It would be good if Congress enacted legislation that modernized this . . . ."↩
13. Clarifying Lawful Overseas Use of Data (CLOUD) Act, Pub. L. No. 115-141, 132 Stat. 348 (2018), § 103(a), (to be codified at 18 U.S.C. § 2713). If, however, the data is not within the company's possession, custody, or control there is no obligation to disclose.↩
14. CLOUD Act § 103(b) (codified at 18 U.S.C. § 2703(h)). If and when applicable, reviewing courts are instructed to consider the location and nationality of the investigative target whose data is being sought, the importance of the data to the investigation, and the relative interests of the United States and relevant foreign government, among other facts.↩
15. That said, the entire point of the executive agreements is, in significant part, to eliminate such conflict, meaning that, even when the set of qualifying governments increases, this statutory mechanism will rarely be invoked if the agreements work as intended.↩
16. CLOUD Act § 103(c).↩
17. The absence of any such conflicts to date undercuts the description of the CLOUD Act as representing a massive expansion of U.S. law enforcement reach and the prediction of increased legal conflict that some suggested would result from allowing U.S. access to data located abroad. See, e.g., Brief for Microsoft Corp. at 13, *United States v. Microsoft Corp.*, 138 S. Ct. 1186 (2018) (No. 17-2), <https://www.supremecourt.gov/DocketPDF/17/17-2/27619/20180111205746909_Brief%20for%20Respondent%202018.01.11.pdf> accessed 12 December 2018 (warning of "direct conflicts with foreign laws that govern emails stored in foreign lands"); *id.* at 41 (same).↩
18. Brief for Ireland as Amicus Curiae in Support of Neither Party, *United States v. Microsoft Corp.*, 138 S. Ct. 1186 (2018) (No. 17-2), <https://www.supremecourt.gov/DocketPDF/17/17-2/23732/20171213152516784 17-2%20ac%20Ireland%20supporting%20neither%20party.pdf> accessed 12 December 2018.↩
19. See Regulation (EU) 2016/679 of the European Parliament and of the Council, *O.J.* L 119, 4.5.2016, 1 [hereinafter GDPR], Arts. 48-49 (laying out transfer restrictions plus exceptions). Whether, to what extent, and in what situations the exceptions to the otherwise applicable transfer restrictions will permit a provider to transfer EU-held data to U.S. law enforcement remains an open question. See *infra* notes 35–38 and accompanying text. That said, the absence of any such conflicts to data undercuts the description of the CLOUD Act as representing a massive expansion of U.S. law enforcement reach and the prediction of increased legal conflict that some suggested would result from allowing U.S. access to data located abroad. See, e.g., Brief for Microsoft Corp. at 13, *United States v. Microsoft Corp.*, 138 S. Ct. 1186 (2018) (No. 17-2), <https://www.supremecourt.gov/DocketPDF/17/172/27619/20180111205746909_Brief%20for%20Respondent%202018.01.11.pdf> accessed 12 December 2018 (warning of "direct conflicts with foreign laws that govern emails stored in foreign lands"); *id.* at 41 (same).↩
20. See G. Kent, "The Mutual Legal Assistance Problem Explained", *CIS Blog* (23 February 2015), <http://cyberlaw.stanford.edu/blog/2015/02/mutual-legal-assistance-problem-explained> (describing the process).↩
21. See R. 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, 2013, <https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf> accessed 12 December 2018, pp. 227–28 (noting that it takes an average of ten months to process these MLAT requests).↩
22. See *Data Stored Abroad: Ensuring Lawful Access and Privacy Protection in the Digital Era: Hearing Before the H. Comm. on the Judiciary*, 115th Cong. (2017) (written statement of Paddy McGuinness, Deputy National Security Adviser, U.K.), <https://docs.house.gov/meetings/JU/JU00/20170615/106117/HHRG-115-JU00-Wstate-McGuinnessP-20170615.pdf> accessed 12 December 2018; *Hearing Before the S. Judiciary Subcomm. on Crime and Terrorism*, 115th Cong. (2017) (written testimony of Paddy McGuinness, Deputy National Security Adviser, U.K.), <https://www.judiciary.senate.gov/imo/media/doc/05-10-17%20McGuinness%20Testimony.pdf> accessed 12 December 2018; see also J. Daskal, "Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues", (2016) 8 *J. Nat'l Sec. L. & Pol'y*, 473, <http://jnslp.com/wp-content/uploads/2017/10/Law-Enforcement-Access-to-Data-Across-Borders_2.pdf> accessed 12 December 2018.↩
23. CLOUD Act § 105(a) (codified at 18 U.S.C. § 2523 (b)(1)).↩
24. *Id*. (codified at 18 U.S.C. § 2523 (b)(4)(D)(ii)- (v)).↩
25. [25] For a further elaboration of these protections, see J. Daskal, *Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0*, (2018) 71 *Stan. L. Rev. Online* 9, 13-15, <https://www.stanfordlawreview.org/online/microsoft-ireland-cloud-act-international-lawmaking-2-0/>; J. Daskal & P. Swire, "Why the CLOUD Act is Good for Privacy and Human Rights", *Just Security* (Mar. 14, 2018), <https://www.justsecurity.org/53847/cloud-act-good-privacy-human-rights/> all accessed 12 December 2018.↩
26. CLOUD Act § 105(a) (codified at 18 U.S.C. § 2523 (b)(4)(D)(vi).↩
27. *Id.* (codified at 18 U.S.C. § 2523 (b)(4)(F)).↩
28. *Id.* (codified at 18 U.S.C. § 2523 (b)(4)(G)).↩
29. *Id.* (codified at 18 U.S.C. § 2523 (b)(4)(J)).↩
30. See Council of the European Union, "Agreement Between the United States of America and the European Union on the Protection of Personal information Relating to the Prevention, Investigation, Detection, and Prosecution of Criminal Offenses", Council doc. 8557/16 of 18 May 2016.↩
31. CLOUD Act § 105(a) (codified at 18 U.S.C. § 2523 (a)(2)); 18 U.S.C § 2523(a)(2)(defining U.S. person).↩
32. *Id.* (codified at 18 U.S.C. § 2523 (b)(4)(A-C)).↩

33. CLOUD Act § 105(a) (codified at 18 U.S.C. § 2523 (b)(4)(I).↩
34. Arts. 48–49 GDPR.↩
35. See, e.g., European Data Protection Board, Guidelines 2/2018 on Article 49 under Regulation 2016/679 (adopted on 25 May 2018), <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf> accessed 12 December 2018.↩
36. See Brief of the European Commission on Behalf of the European Union as Amicus Curiae in Support of Neither Party, *United States v. Microsoft Corp.*, 138 S. Ct. 1186 (2018) (No. 17-2), <https://www.supremecourt.gov/DocketPDF/17/17-2/23655/20171213123137791_17-2%20ac%20European%20Commission%20for%20filing.pdf> accessed 12 December 2018, pp. 12–16 (noting the data transfer restrictions included in the GDPR, highlighting the possibility that transfers could be justified under Art. 49 of the Regulation, but also emphasizing that Art. 49 grounds for transfer are to be "interpreted strictly").↩
37. For a further discussion of this issue, see J. Daskal, "Microsoft Ireland, the CLOUD Act, and International Lawmaking *2.0*", (2018) 71 *Stan. Online Rev.*, 9, 12–13.↩
38. See also P. Swire and J. Hemmings, "Recommendations for the Potential US-UK Executive Agreement Under the CLOUD Act", *Lawfare (13 September 2018)*, <https://www.lawfareblog.com/recommendations-potential-us-uk-executive-agreement-under-cloud-act> accessed 12 December 2018 (suggesting additional provisions).↩
39. See J. Daskal, "Setting the Record Straight: The CLOUD Act & The Reach of Wiretapping Authority Under US Law", *CBDF Forum* (15 October 2017), <https://www.crossborderdataforum.org/setting-the-record-straight-the-cloud-act-and-the-reach-of-wiretapping-authority-under-us-law/> accessed 12 December 2018.↩
40. See also T. Wahl, "Commission Proposes Legislative Framework for E-Evidence", *eucrim* 1/2018, 35-36; For a detailed analysis, see the article of S. Tosza, in this issue.↩
41. See Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) (Austl.), Sch. 1 § 317C (defining scope of coverage), <https://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/r6195_aspassed/toc_pdf/18204b01.pdf;fileType=application/pdf> accessed 17 January 2019.↩
42. Hof van Cassatie [Cass.] [Court of Cassation], 18 January 2011, *Procureur-Général v. Yahoo! Inc.,* Nr. P.10.1347.N (Belg.), translated in: (2011) 8 *Digital Evidence & Electronic Signature L. Rev.* 216, 216–18, <http://journals.sas.ac.uk/deeslr/article/view/1978/1915> accessed 12 December 2018; see Hof van Beroep [HvB] [Court of Appeal] Antwerp, Nov. 15, 2017, *Openbaar Ministerie v. Skype Commc'ns SARL,* 2016/CO/1006 (Belg.), 5.1.1.4., 5.1.2.2. For a further discussion of these cases and related issues, see J. Daskal, "Borders and Bits", (2017) 71 *Vand. L. Rev.,* 101, 114–118.↩

About eucrim

eucrim is the leading journal serving as a European forum for insight and debate on criminal and "criministrative" law. For over 20 years, it has brought together practitioners, academics, and policymakers to exchange ideas and shape the future of European justice. From its inception, eucrim has placed focus on the protection of the EU's financial interests – a key driver of European integration in "criministrative" justice policy.
Editorially reviewed articles published in English, French, or German, are complemented by timely news and analysis of legal and policy developments across Europe.
All content is freely accessible at https://eucrim.eu, with four online and print issues published annually.

Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases.
The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by the European Union