PRIVACY — STORED COMMUNICATIONS ACT — SECOND CIRCUIT HOLDS THAT THE GOVERNMENT CANNOT COMPEL AN INTERNET SERVICE PROVIDER TO PRODUCE INFORMATION STORED OVERSEAS. — *Microsoft Corp. v. United States*, 829 F.3d 197 (2d Cir. 2016).

Nearly all Internet users interact with "the cloud" every day, but most never consider what — or where — "the cloud" is.[1] As it turns out, "the cloud" is composed of server farms[2] located all over the world.[3] Companies like Google, Facebook, Apple, Microsoft, and Amazon now host large quantities of data abroad,[4] raising novel jurisdictional questions. Recently, in *Microsoft Corp. v. United States*,[5] the Second Circuit held that the government cannot compel Internet Service Providers (ISPs) to turn over data stored overseas, even with a warrant.[6] The court did not acknowledge the unique "un-territorial" nature of data, instead proceeding as if it were considering a physical object. Increasingly, courts must apply old laws to new technology. In doing so, they can either acknowledge the unique features of modern technology, or, like the Second Circuit, they can disregard these differences. Only the first approach allows courts to grapple with the legal issues generated when old law meets new tech.[7] In *Microsoft*, the majority did not engage with the emerging scholarly consensus that the "where" of data is not a straightforward inquiry.[8] It thus did not address the novel issues implicated in this case and failed to reason through its decision fully.

[1] *See* Damon C. Andrews & John M. Newman, *Personal Jurisdiction and Choice of Law in the Cloud*, 73 MD. L. REV. 313, 324 (2013).

[2] Steven R. Swanson, *Google Sets Sail: Ocean-Based Server Farms and International Law*, 43 CONN. L. REV. 709, 714 (2011). "[A] server is a computer designed to provide information or processes to other computers on a network, and a server farm, also known as a data center, is a group of servers in one location connected by a network." *Id.* (citations omitted).

[3] *See, e.g.*, *Data Center Locations*, GOOGLE, https://www.google.com/about/datacenters/inside/locations/index.html [https://perma.cc/V6ZH-YPD7] (noting that Google, a cloud service provider, has fifteen server farms across the Americas, Asia, and Europe).

[4] *See, e.g.*, *id.*

[5] 829 F.3d 197 (2d Cir. 2016).

[6] *Id.* at 222.

[7] *See, e.g.*, Zachary D. Clopton, *Territoriality, Technology, and National Security*, 83 U. CHI. L. REV. 45, 52 (2016).

[8] Scholarship questioning whether the physical location of data is a meaningful concept includes, for example, Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326, 390 (2015); Andrews & Newman, *supra* note 1, at 372–73; Clopton, *supra* note 7, at 46; David R. Johnson & David Post, *Laws and Borders — The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1376 (1996); and Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. PA. L. REV. 373, 408 (2014). For an opposing view, see Andrew Keane Woods, *Against Data Exceptionalism*, 68 STAN. L. REV. 729 (2016).

In December of 2013, Magistrate Judge Francis of the Southern District of New York issued a warrant under the Stored Communications Act[9] (SCA) for the content associated with a Microsoft Network (MSN) email address.[10] Microsoft handed over responsive data stored in the United States.[11] However, much of the requested information was stored on a Microsoft server in Ireland.[12] Believing the data in Ireland to be beyond the jurisdiction of the warrant, Microsoft moved to quash the warrant.[13]

The magistrate judge denied the motion, and Judge Preska affirmed for the Southern District.[14] The court noted that a traditional search warrant cannot be executed outside of the United States,[15] but that the language of the SCA is ambiguous regarding jurisdiction.[16] An SCA warrant, the court reasoned, is a hybrid between a search warrant and a subpoena.[17] Its subpoena-like qualities supported the government's position — a subpoena recipient must hand over information it controls no matter where that information is located.[18] The practical consequences of its decision bolstered the court's conclusion: letting Microsoft withhold the data stored in Ireland would allow criminals to evade SCA warrants by forcing the government to rely solely on Mutual Legal Assistance Treaties (MLATs) to obtain information stored abroad.[19] This could not have been Congress's intention — MLATs are slow and unreliable, and many countries have no MLAT with the United States.[20] Finally, the court noted "the concerns that animate the presumption against extraterritoriality are simply not present" in this case.[21]

[9] 18 U.S.C. §§ 2701–2712 (2012).

[10] *Microsoft*, 829 F.3d at 200.

[11] *Id.*

[12] *Id.* at 200–01.

[13] *In re* Warrant to Search a Certain E-mail Account Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 466, 470 (S.D.N.Y. 2014).

[14] *Microsoft*, 829 F.3d at 201.

[15] *See* FED. R. CRIM. P. 41(b)(5).

[16] *See Warrant to Search*, 15 F. Supp. 3d at 470.

[17] Like a search warrant, an SCA warrant is issued by a neutral magistrate under a showing of probable cause. *Id.* at 471. Like a subpoena, it is the recipient of the warrant, not law enforcement agents, who produces the sought-after information. *Id.*

[18] *Id.* at 471–72.

[19] *Id.* at 474. MLATs are international agreements to share information and evidence between law enforcement authorities. *See* UNITED NATIONS OFFICE ON DRUGS & CRIME, MANUAL ON MUTUAL LEGAL ASSISTANCE AND EXTRADITION 19 (2012).

[20] *See Warrant to Search*, 15 F. Supp. 3d at 474–75.

[21] *Id.* at 475; *see also id.* at 475–76 ("[A]n SCA Warrant does not criminalize conduct taking place in a foreign country; it does not involve the deployment of American law enforcement personnel abroad; it does not require even the physical presence of service provider employees at the location where data are stored. At least in this instance, it places obligations only on the service provider to act within the United States.").

The Second Circuit reversed. Writing for the majority, Judge Carney[22] held that the SCA does not apply extraterritorially, and that requiring Microsoft to turn over the disputed data would constitute an extraterritorial application of the statute.[23]

Applying the two-part test for extraterritoriality laid out by the Supreme Court, the court first concluded that the SCA does not apply extraterritorially.[24] The court found no indication of Congress's intent to override the strong presumption against the extraterritorial application of statutes.[25] Further, the court held that the word "warrant" was a term of art, whose meaning was tied to Fourth Amendment search warrants that "protect[] privacy in a distinctly territorial way."[26] The court rejected the government's argument that an SCA warrant is a search warrant/subpoena hybrid: the SCA itself distinguishes between subpoenas and warrants,[27] and nowhere uses the word "hybrid."[28]

Second, the court held that compelling Microsoft to turn over the data stored in Ireland would be an extraterritorial application of the SCA.[29] To reach this conclusion, the court had to determine the "focus" of the SCA's warrant provision.[30] If the "domestic contacts" of the case did not fall within the focus of the SCA, then the warrant would constitute an extraterritorial application of the statute.[31] The court concluded that the focus of the SCA was protecting privacy.[32] The court supported this conclusion by pointing to the SCA's reference to the federal rule governing traditional search warrants,[33] and to the fact that the SCA was passed as part of the Electronic Communications Privacy Act, with the word "privacy" in its very title.[34] The court further noted that the SCA protects privacy in a variety of contexts unrelated to government requests, which undermined the government's claim that the statute's focus was aiding law enforcement.[35]

[22] Judge Carney was joined by District Judge Bolden, sitting by designation from the District of Connecticut.

[23] *Microsoft*, 829 F.3d at 222.

[24] *Id.* at 210 (citing Morrison v. Nat'l Austl. Bank Ltd., 561 U.S. 247, 261–70 (2010)). The *Morrison* test first looks to the statutory text for a clear indication of intent to apply extraterritorially, and if no such clear statement is found, it examines the facts to determine whether the proposed use of the statute would be extraterritorial. *Morrison*, 561 U.S. at 261–70.

[25] *Microsoft*, 829 F.3d at 216.

[26] *Id.* at 212.

[27] *Compare* 18 U.S.C. § 2703(b)(1)(B)(i), (c)(2) (2012) (requiring a *subpoena*), *with* 18 U.S.C. § 2703(a) (requiring a *warrant*).

[28] *Microsoft*, 829 F.3d at 214.

[29] *Id.* at 220.

[30] *Id.* at 216 (quoting Mastafa v. Chevron Corp., 770 F.3d 170, 183 (2d Cir. 2014)).

[31] *Id.* (citing Morrison v. Nat'l Austl. Bank Ltd., 561 U.S. 247, 267 (2010)).

[32] *Id.* at 217.

[33] *Id.* (citing FED. R. CRIM. P. 41).

[34] *Id.*

[35] *Id.* at 217–18.

Since the SCA's focus was privacy, and the privacy interest was in Ireland, compelling Microsoft to turn over the data in question would be an extraterritorial, and thus unlawful, application of the SCA.[36]

Judge Lynch concurred in the judgment.[37] He began by stressing what the case was *not* about: privacy.[38] A warrant, issued by a neutral magistrate under a showing of probable cause, is the "highest level of protection ordinarily required by the Fourth Amendment."[39] Judge Lynch doubted that privacy interests would be better protected by "the business decision[] of a private corporation" than by "the traditional constitutional safeguard" of a search warrant.[40]

For Judge Lynch, the case boiled down to a dispute over the "international reach of American law."[41] He agreed with the majority that the SCA contained no indication that it should apply extraterritorially.[42] He went a step further than the majority as to *why* that was so: in 1986, the year it passed the SCA, Congress could not have foreseen the developments of modern cloud technology.[43] Due to the nature of cloud technology, whether compelling disclosure of the data stored in Ireland would constitute an extraterritorial application of the SCA was a very close question. After all, data in the cloud is not nearly as physically moored as tangible objects, and "[t]he entire process of compliance [with the warrant would] take[] place domestically" with a few clicks on a computer.[44] But because the nationality of the account holder was unknown and that person may not have been from the United States, Judge Lynch ultimately did not believe that Congress wanted "to reach situations of this kind."[45] The warrant was thus an unlawful extraterritorial application of the SCA.[46]

When courts must apply old laws to modern technology, they face a choice: they can treat technology as they would anything else, or they can acknowledge its unique qualities and consider adapting their application of existing laws accordingly. The trouble with choosing the

[36] *Id.* at 220.

[37] *Id.* at 222 (Lynch, J., concurring in the judgment).

[38] *Id.*

[39] *Id.* at 223.

[40] *Id.* at 224 ("[N]either privacy interests nor the needs of law enforcement vary depending on whether a private company chooses to store records here or abroad — particularly when the 'records' are [data] that can be moved around the world in seconds, and *will* be so moved whenever it suits the convenience or commercial purposes of the company." *Id.*).

[41] *Id.* at 225.

[42] *Id.* at 226.

[43] *Id.* at 231. Judge Lynch noted that Congress's lack of foresight does not permit courts to create intention where none existed. *Id.* at 226.

[44] *Id.* at 229.

[45] *Id.* at 230.

[46] *Id* at 230–31. The concurrence concluded by noting that the SCA was an outdated law that required the attention of Congress. *Id.* at 231–32.

former, as the *Microsoft* court did, is that "[a] law created for one world may have a very different impact when applied to the facts of a different era."[47] When courts ignore the technological elephant in the room, they risk failing to evaluate the novel issues that arise with modern technology — issues that might require an adjustment to existing legal doctrine. In this case, after the majority concluded that the SCA could not be applied extraterritorially, it had "little trouble concluding that the execution of the [w]arrant would constitute an unlawful extraterritorial application of the [SCA]."[48] The court did not consider how the application of the presumption against extraterritoriality to data might differ from its application to a physical object, therein overlooking the growing scholarly debate over this question. Reasonable minds may disagree whether the court's ultimate conclusion was correct, but the court's failure to consider the unique attributes of data reflects incomplete reasoning getting there. In essence, the court skipped a step, because it didn't think to check whether the step was there.

Microsoft was decided in the context of deep uncertainty regarding the territoriality of data among legal scholars[49] and ISPs[50] alike. Many commentators have concluded that "the very idea of online data being located in a particular physical 'place' is becoming rapidly outdated."[51] According to Professor Jennifer Daskal, the utility of "territorial-based dividing lines" depends on two assumptions: "that objects have an identifiable and stable location," and that "location matters."[52] Cloud-stored data undermines both assumptions. First, data moves around the world quickly,[53] often fragmented and stored on multiple servers.[54] Second, the "disconnect between the location of data and the location of its user" means that data's "location" should not hold much significance.[55] Because the whereabouts of cloud-

[47] Orin S. Kerr, *Foreword: Accounting for Technological Change*, 36 HARV. J.L. & PUB. POL'Y 403, 403 (2013).

[48] *Microsoft*, 829 F.3d at 220.

[49] *See* sources cited *supra* note 8.

[50] Several tech giants filed amicus briefs in support of Microsoft. *See, e.g.*, Brief in Support of Appellant Microsoft, Inc. by Apple, Inc. as Amicus Curiae, *Microsoft*, 829 F.3d 197 (No. 14-2985). Google and Facebook are notably missing from this group, likely because both have argued that the "relevant jurisdictional hook . . . ought to be the domicile of the corporation." Woods, *supra* note 8, at 736 n.29. However, Google has also argued that the key to jurisdiction is the location of the server on which the requested data resides. *See* Erika Morphy, *Google, Brazil Lock Horns Over Social Networking Data*, TECHNEWSWORLD (Aug. 24, 2006), http://www.technewsworld.com/story/privacy/52624.html [https://perma.cc/GE5N-2QNU].

[51] Kerr, *supra* note 8, at 408; *see also* sources cited *supra* note 8.

[52] Daskal, *supra* note 8, at 329.

[53] *See id.*; *see also* Clopton, *supra* note 7, at 52.

[54] *See* Andrews & Newman, *supra* note 1, at 316–17; Kerr, *supra* note 8, at 408.

[55] Daskal, *supra* note 8, at 329; *see also* Clopton, *supra* note 7, at 49.

stored data is out of the user's control — and often information that is not even available to the user — the notion that the location of data would matter more than the location of the person creating the data simply does not make much sense.[56] In sum, data is what Daskal calls "un-territorial."[57]

The *Microsoft* majority did not acknowledge the "un-territorial" nature of data. In fact, the court only briefly referred to the notion that cloud-stored data differs from the traditional objects of search warrants and dismissed the importance of this fact out of hand: "Although electronic data may be more mobile, and may seem less concrete, than many materials ordinarily subject to warrants, no party disputes that the electronic data subject to this [w]arrant [are] in fact located in Ireland . . . ."[58] The rest of the opinion discussed data in a manner interchangeable with physical objects, speaking of the collection, storage, and location of the information abroad.[59] In fairness to the court, it did acknowledge that the world has changed since the passage of the SCA, and indicated that it felt constrained by an outdated statute.[60] Yet *Microsoft* was not simply a matter of the court straightforwardly applying an outdated statute. As Daskal noted in her comments on the district court's decision in this case: "[I]t is clear that a territorial presumption applies to the SCA. But the question of *how* this presumption applies when an international border separates the data and the person or entity accessing the data remains unsettled."[61] It is this second question that the majority did not engage with. Because it did not consider the unique attributes of data, the court ignored the emerging consensus that placing much importance on the "location" of data is a mistake.

Microsoft is not the first time that a court has failed to grapple with legal wrinkles created by new technology. One prominent example is *Olmstead v. United States*,[62] in which the Supreme Court held that a wiretap did not constitute a search under the Fourth Amendment.[63] Traditional Fourth Amendment doctrine held that a physical trespass was required in order for the government's action to consti-

[56] *See* Daskal, *supra* note 8, at 329.

[57] *Id.* at 397.

[58] *Microsoft*, 829 F.3d at 209; *see also id.* at 220 n.28.

[59] *See, e.g.*, *id.* at 209 (noting that the data in question "were in fact *located* in Ireland," *id.* (emphasis added), that "Microsoft would have to *collect* the data from Ireland," *id.* (emphasis added), and that the data were "*stored* in Dublin," *id.* at 220 (emphasis added)).

[60] *See id.* at 201. Indeed, perhaps some fault lies with Congress, which has not updated the SCA to address the "un-territorial" nature of data. *See id.* at 231–32 (Lynch, J., concurring in the judgment).

[61] Daskal, *supra* note 8, at 363.

[62] 277 U.S. 438 (1928).

[63] *Id.* at 464.

tute a search.[64] Instead of considering the novel attributes of modern technology and adjusting the definition of a search accordingly, the Court simply applied the trespass test and determined that a wiretap could not amount to a search.[65] Not only was this incomplete legal reasoning, but it also resulted in a significant delay in developing Fourth Amendment doctrine appropriate for modern technology. It was not until *Katz v. United States*,[66] decided nearly forty years later, that the Court created an additional definition of a search appropriate for modern technology — the expectation-of-privacy test.[67]

Microsoft may be a new *Olmstead*. Like in *Olmstead*, the *Microsoft* majority failed to appreciate the unique attributes of new technology, and as a result the court did not recognize that its application of existing legal doctrine may have required an additional step.

By skipping over the question of how territoriality applies to data, the court did not fully reason through a decision with policy consequences that are, at the very least, bizarre. According to the Second Circuit, law enforcement is absolutely barred from obtaining electronic communications stored abroad directly from an ISP. The only recourse the government has is appealing to MLATs,[68] which are notoriously slow[69] and do not exist with every country.[70] Even if the crime were entirely local — a U.S. defendant committed a crime against a U.S. victim on U.S. soil — with the only international component being an ISP's business decision to store the defendant's emails abroad, the government now has *no means* by which to compel disclosure of what could be critical evidence directly from the ISP. The concurrence rightfully recognized the oddity of this outcome, noting "it would be remarkably formalistic to classify such a demand as an extraterritorial application of what is effectively the subpoena power of an American court."[71] Even Microsoft acknowledges that this is not a favorable state of affairs, expressing its support[72] for the International Commu-

[64] *See* Katz v. United States, 389 U.S. 347, 353 (1967).

[65] *Olmstead*, 277 U.S. at 464; *see also Katz*, 389 U.S. at 353.

[66] 389 U.S. 347.

[67] *See id.* at 360–61 (Harlan, J., concurring).

[68] *Microsoft*, 829 F.3d at 221.

[69] *See, e.g.*, Jennifer Daskal, *A New UK-US Data Sharing Agreement: A Tremendous Opportunity, if Done Right*, JUST SECURITY (Feb. 8, 2016, 8:10 AM), https://www.justsecurity.org/29203/british-searches-america-tremendous-opportunity [https://perma.cc/U2ZX-AAJQ] (noting that, under the U.K.-U.S. MLAT, U.K. data requests to the United States take ten months to process, on average).

[70] For a list of U.S. MLATs, see *2016 INCSR: Treaties*, U.S. DEP'T OF STATE, http://www.state.gov/j/inl/rls/nrcrpt/2016/vol2/253357.htm [https://perma.cc/D8XE-L9F9].

[71] *Microsoft*, 829 F.3d at 230 (Lynch, J., concurring in the judgment).

[72] Bob Van Voris & Dina Bass, *Microsoft Wins Protection for E-mails Stored Outside U.S.*, BLOOMBERG TECH. (July 14, 2016, 10:48 AM), http://www.bloomberg.com/news/articles

nications Privacy Act, which would allow law enforcement officials to obtain electronic communications "*regardless of where those communications are located*," pursuant to a warrant.[73]

Of course, it is entirely possible that the court would have considered the "un-territoriality" of data and still decided for Microsoft, similar to the position of the concurring opinion.[74] There would have been good reasons for them to do so. First, the debate over the territorial nature of data is just that — a debate. There are those who believe that "despite the wizardry and wonder of modern technological advances, cloud-based data is not conceptually novel enough" to be deemed exceptional.[75] Second, the presumption against extraterritoriality exists, in part, because the "extraterritorial application [of U.S. laws] may offend foreign governments,"[76] and it is clear that at least some foreign officials were offended by the government's position in *Microsoft*.[77] Third, deciding in favor of the government would have had negative policy implications of its own.[78] Indeed, Daskal herself has noted that *neither* position in this case is "satisfying,"[79] but even so the majority may have come to the "correct" conclusion.[80]

The *Microsoft* court, as courts are trained to do, applied the words of the statute and relevant precedent to the issue at hand. But with advances in technology, rote application of existing legal doctrine is not enough. At best, the *Microsoft* court accidently arrived at the right decision. At worst, the court issued an *Olmstead*, and missed the chance to adapt legal doctrine to modern technology. If this is the case, hopefully the correction does not take forty years to surface.

/2016-07-14/microsoft-wins-appeal-in-case-over-customers-e-mail-security [https://perma.cc/TT2R-ZVNE].

[73] Press Release, Senator Orrin Hatch, Hatch, Coons, Heller Introduce Bipartisan International Communications Privacy Act (May 25, 2016) (emphasis added), http://www.hatch.senate.gov/public/index.cfm/2016/5/hatch-coons-heller-introduce-bipartisan-international-communications-privacy-act [https://perma.cc/PZ86-V5JL].

[74] *Microsoft*, 829 F.3d at 230–31 (Lynch, J., concurring in the judgment).

[75] Woods, *supra* note 8, at 734.

[76] William S. Dodge, *Understanding the Presumption Against Extraterritoriality*, 16 BERKELEY J. INT'L L. 85, 121 (1998) (quoting Curtis A. Bradley, *Territorial Intellectual Property Rights in an Age of Globalism*, 37 VA. J. INT'L L. 505, 562 (1997)).

[77] *See* Brief of Amicus Curiae Jan Philipp Albrecht, Member of the European Parliament, *Microsoft*, 829 F.3d 197 (No. 14-2985).

[78] *See* Daskal, *supra* note 8, at 397 ("[A] win for the government would establish a dangerous precedent under which nations can unilaterally . . . compel the production of data located anywhere in the world simply by asserting jurisdiction over the company controlling the data.").

[79] Jennifer Daskal, *The Microsoft Warrant Case: The Policy Issues*, JUST SECURITY (Sept. 8, 2015, 12:48 PM), https://www.justsecurity.org/25901/microsoft-warrant-case-policy-issues [https://perma.cc/LY7P-KM9N].

[80] Jennifer Daskal, *Three Key Takeaways: The 2d Circuit Ruling in the Microsoft Warrant Case*, JUST SECURITY (July 14, 2016, 6:28 PM), https://www.justsecurity.org/32041/key-takeaways-2d-circuit-ruling-microsoft-warrant-case [https://perma.cc/2ADU-GDEK].