MICROSOFT V. UNITED STATES: IN THE MATTER OF A WARRANT TO SEARCH A CERTAIN E–MAIL ACCOUNT CONTROLLED AND MAINTAINED BY MICROSOFT CORPORATION

Jeffery Gary[*] & Jane Olin-Ammentorp[•]

CITE AS: 1 GEO. L. TECH. REV. 52 (2016)

https://perma.cc/QN57-RLQC

INTRODUCTION

As technology continues to evolve, the need to provide meaningful consumer protections remains an immense challenge for legislators and jurists. Aging statutes and inadequate precedents make devising modern technological solutions difficult.[1] Increasingly, courts have had difficulty grappling with the questions arising from the increasing volume of consumer data, particularly how to consider the implications of data in the hands of third parties.[2] This difficulty becomes especially acute when applied to data flows and Internet

[*] Assistant Case Comments Editor, GLTR; Georgetown Law, J.D. expected 2018; J.D.; King's College London, M.A. 2014; DePaul University, B.F.A. 2012.

[•] GLTR Staff Member; Georgetown Law, J.D. expected 2018; University of Oxford, M.Sc. 2011; Cornell University, B.A. 2009.

[1] *See, e.g.* Kyllo v. United States, 533 U.S. 27 (2001); United States v. Jones, 132 S.Ct. 945 (2012) (Sotomayor, J., concurring) ("More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.") (internal citations omitted).

[2] *See* In re Pharmatrak, Inc., 329 F.3d 9 (1st Cir. 2003) (applying Wiretap Act to find no interception when a website directs a user's browser to make third-party cookie requests).

traffic, which defy simple categorization.[3] Recently, in *Microsoft v. United States*, the Second Circuit held that U.S. law enforcement may not compel a domestic data processing company to provide data that is stored outside the country.[4]

This comment will explain that the Second Circuit correctly applied existing law, but failed to understand the technological underpinnings and statutory intent at issue. To do so, the comment will discuss the history of the Electronic Communications Privacy Act (ECPA), including the development of the statute's warrant provisions, and original intent to protect individual privacy and civil liberties. The comment will further show that in the years since ECPA's enactment, new technology has diminished the ability of the statute to provide meaningful guidance for law enforcement. It will then discuss the court's holding, and analyze why the court has misconstrued the nature of the data at issue, even though the court correctly applied the existing law. The comment will conclude with thoughts on the impact this holding may have on technology companies and consumers, and address concerns rising from the increasing trend of data localization.

STATUTORY BACKGROUND AND PROCEDURAL HISTORY

The Stored Communications Act (SCA) was enacted in 1986 as Title II of ECPA.[5] ECPA replaced the Wiretap Act, which was part of the Omnibus Crime Control and Safe Streets Act of 1968.[6] ECPA was intended to modernize the legal framework for surveillance as new technologies such as computer communication outpaced the civil liberties protections already in place.[7] Though ECPA was passed before the mass proliferation of web services,

---

[3] *See* Katitza Rodriguez, *Colombian Users to ISPs: 'Where Is My Data?'*, ELEC. FRONTIER FOUND. (May 20, 2015), https://www.eff.org/deeplinks/2015/05/which-internet-providers-tell-colombians-where-their-data.

[4] In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 829 F.3d 197 (2d Cir. 2016) [hereinafter "Microsoft"].

[5] Electronic Communications Privacy Act, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. § 2701 *et seq.* (1986)).

[6] Omnibus Crime Control and Safe Streets Act, Pub. L. No. 90-351, 801, 82 Stat. 197, 212 (1968).

[7] 130 CONG. REC. 4107-08 (Oct. 1, 1984) (Remarks of Rep. Kastenmeier introducing ECPA in the House of Representatives), https://www.justice.gov/sites/default/files/jmd/legacy/2014/08/26/cr-e4107-08-1984.pdf; 131 CONG. REC. 24365-71 (Sept. 19, 1985) (Remarks of Sen. Leahy introducing ECPA in the Senate), https://www.justice.gov/sites/default/files/jmd/legacy/2014/07/11/cr-24365-71-1985.pdf.

ECPA's provisions have been interpreted to cover email,[8] private social media messages,[9] and text messages.[10]

Section 2703 of the SCA authorizes law enforcement to variously obtain court orders, subpoenas, or warrants compelling private companies to disclose user data. The disclosure mechanisms operate in a tiered system: court orders require the lowest standards for evidence, but only allow access to customer record information.[11] Subpoenas require an equivalent level of reasonable suspicion, and allow law enforcement to view non-content data of specific messages.[12] The highest level of protection is provided for the contents[13] of communications in electronic storage that have been stored for 180 days or fewer.[14] To access such data, law enforcement must obtain an SCA warrant consistent with the Federal Rules of Criminal Procedure, including a showing of probable cause to a magistrate judge.[15] Each mechanism also allows access to the information obtainable by a lesser degree of proof in a sliding scale: law enforcement officials could obtain a warrant and see all the information available through a court order, for example.[16]

In *Microsoft*, the FBI obtained a warrant—subject to the strictest requirements of § 2703—to compel the company to disclose the email record information and email content of an account that had allegedly been used in furtherance of narcotics trafficking.[17] Microsoft complied with the portion of the request for the account's non-content information, which was stored in the United States, but refused to comply with the request for content data, arguing

[8] Theofel v. Farey-Jones, 359 F.3d 1066, 1077 (9th Cir. 2003).
[9] *See* Crispin v. Christian Audigier, 717 F. Supp. 2d 965, 980, 989 (C.D. Cal. 2010).
[10] *See* Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892, 901 (9th Cir. 2008).
[11] 18 U.S.C. § 2703(c)(B) (2012).
[12] 18 U.S.C. § 2703(d) (2012).
[13] Content is generally defined as the intended message defined by the communication, while information used to address or process the message (i.e. addressing or timestamp information) is considered non-content, and afforded lower levels of protection, even when it may contain sensitive information. *See* In re Zynga Privacy Litigation, 750 F.3d 1098, 1106 (9th Cir. 2014) ("Congress intended the word 'contents' to mean . . . the essential part of the communication, the meaning conveyed, and the thing one intends to convey.") (internal marks omitted).
[14] 18 U.S.C. § 2703(a)–(b) (2012).
[15] 28 U.S.C. § 2703(a) (2012); *see* FED. R. CRIM. P. Rule 41. A warrant under § 2703 requires a showing of specific and articulable facts showing reasonable grounds to believe that the contents, records, or other information in or relating to a wire or electronic communication are relevant and material to an ongoing criminal investigation. § 2703(b)(1)(B) of ECPA generally requires providing notice to a subscriber to get contents of communications, though this is not always the case when accessing records.
[16] *See* 18 U.S.C. § 2703(c) (2012).
[17] *Microsoft*, 829 F.3d 197, 202–3 (2d Cir. 2016).

that as the information was stored and maintained in Ireland, and the government had not established that the target of the investigation was a U.S. national, the information was not subject to U.S. jurisdiction.[18]

Microsoft moved to quash the warrant; however, the District Court denied the motion and held Microsoft in civil contempt for its failure to comply with the warrant.[19] Microsoft appealed and the Second Circuit court reversed and vacated the District Court's contempt holding.[20]

TECHNOLOGICAL HISTORY

ECPA was enacted in 1986, well before the internet became a ubiquitous feature of everyday interactions. The "sophisticated technology" that prompted the enactment of ECPA in the mid-1980s included video surveillance and information passing over telephone lines.[21] The legal issues flowing from these new technologies largely hinged on whether the government could legally access communication data owned by a particular person and stored in a particular place.[22] At the time of enactment, the familiar analogy between postal mail and email still held strong: an individual sent a communication, it was transmitted by the individual's provider, and then collected by the individual's intended recipient. The email was stored on the personal computers of the two correspondents, and only stored by a provider if a correspondent specifically signed up for that service.[23]

In *Microsoft*, the service at issue is Outlook, the familiar email client. Microsoft administers the service through an international network of servers in over 100 countries.[24] An Outlook user's data is stored in servers nearest the user, in order to reduce overall latency and increase the efficiency of the service.[25] Messagesare transmitted and stored nearly instantaneously, and

[18] *Id.* at 204.
[19] *Id.* at 205.
[20] *Id.*
[21] *See* Remarks of Rep. Kastenmeier, *supra* note 7.
[22] *See* Remarks of Sen. Leahy, *supra* note 7. ("[T]here is no adequate Federal legal protection against the unauthorized access of electronic communications system computers to obtain or alter the communications contained in those computers.").
[23] It was in this context that the ECS/RCS distinction codified in ECPA arose. This distinction is now largely technologically obsolete, since messages can, as a technological matter, be both stored and transmitted simultaneously, *see* Andrew Keane Woods, *Against Data Exceptionalism*, 68 STAN. L. REV. 4, 729 (2016).
[24] *Microsoft*, 829 F.3d 197, 202–3 (2d Cir. 2016).
[25] *Id.* at 202. ("Microsoft generally stores a customer's e-mail information and content at datacenters located near the physical location identified by the user as its own when

individuals rely on third-party electronic storage solutions to a degree never contemplated in 1986.

Now, email may be drafted, sent, and stored all in the cloud.[26] A provider may be based, or—as in *Microsoft*—store data in a jurisdiction that may or may not be the same jurisdiction where the user resides. The reference in the SCA to the Federal Rules allows the government to receive data stored outside an individual's district; however, the Federal Rules are silent on issues of international storage. [27] The limitations cloud computing places on law enforcement have been addressed forcefully by the courts, which have found, for instance, that law enforcement may not use a search incident to lawful arrest to view information on a phone stored in the cloud. [28]

While the privacy interests implicated in the rise of cloud computing are significant, the challenges to law enforcement are similarly daunting. As more data is stored in the cloud, records that would have been accessible ten years ago to law enforcement with the use of a legitimate warrant are now rendered inaccessible because of technological changes. Storage policies of individual companies might include different protocols about how, where, and whether data is stored, creating an inconsistent set of protections and allowances for consumers and law enforcement. [29] Individuals and their data cross borders with increasing frequency, and there is limited clarity, both in the United States and

---

subscribing to the service. Microsoft does so, it explains, in part to reduce network latency—i.e., delay—inherent in web-based computing services and thereby to improve the user's experience of its service.") (internal quotations omitted); *id.* at 202 n.5 ("[T]he greater the geographical distance between a user and the datacenter where the user's data is stored, the slower the service.").

[26] IBM, *What Is Cloud Computing?*, IBM CLOUD, https://www.ibm.com/cloud-computing/learn-more/what-is-cloud-computing (last visited Nov. 17, 2016) ("Cloud computing, often referred to as simply "the cloud," is the delivery of on-demand computing resources—everything from applications to data centers—over the Internet.").

[27] *See* FED. R. CRIM. P. Rule 41(b)(5). At the time of publication, Congress was considering an amendment to this rule, set to take place Dec. 1, 2016. The amendment would guarantee judicial review for remote warrants under two narrow circumstances: when a suspect has technologically masked his computer, and when a computer crime involves five or more jurisdictions. Leslie R. Caldwell, *Rule 41 Changes Ensure a Judge May Consider Warrants for Certain Remote Searches*, U.S. DEP'T OF JUST.: JUSTICE BLOGS (June 20, 2016), https://www.justice.gov/opa/blog/rule-41-changes-ensure-judge-may-consider-warrants-certain-remote-searches.

[28] Riley v. California, 134 S.Ct. 2473, 2491 (2014).

[29] *See, e.g.*, *Where your data is located*, MICROSOFT TRUST CTR., https://www.microsoft.com/en-us/trustcenter/Privacy/Where-your-data-is-located (last visited Oct. 21, 2016).

abroad, on how territorial boundaries affect data and the substantive rights of its owners.

ANALYSIS

The Second Circuit based its decision on a two-step inquiry. First, after noting the presumption against extraterritorial application of U.S. laws,[30]the court examined whether Congress intended for the SCA to apply extraterritorially. It determined that due to the lack of clear language establishing extraterritorial intent, the statute could not be read to include application outside the United States.[31] This was particularly true, in the court's analysis, as the warrant provisions specifically describe procedures for operation in various U.S. jurisdictions, but none for foreign application.[32] Second, after determining Congress did not intend the SCA to apply extraterritorially, the court concluded that the intent of the SCA was to protect individual privacy by shielding user content from intrusion, rather than to benefit law enforcement.[33] The court held that as the purpose of the law was to protect user information, construing the statute to apply extraterritorially without clear statutory language was inappropriate, since doing so would undermine the original goals of the statute.

However, this holding largely rests on the legal analysis of technological issues that did not exist at the time Congress enacted the SCA, a point emphasized in Judge Lynch's concurrence: "there is no evidence that Congress has *ever* weighed the costs and benefits of authorizing court orders of the sort at issue in this case."[34] Further, as Judge Lynch argued, the characterization "that this case involves a government threat to individual privacy," as was suggested by a number of amici briefs, is largely misguided.[35]

---

[30] Generally, there is a presumption against extraterritorial application of U.S. law, unless a statute specifically notes an alternative intention. *See, e.g.* E.E.O.C. v. Arabian Am. Oil Co., 499 U.S. 244 (1991); Morrison v. Nat'l Austl. Bank, 561 U.S. 247 (2010).

[31] *Microsoft*, 829 F.3d 197, 210 (2d Cir. 2016).

[32] *Id.* at 211 ("We think it particularly unlikely that, if Congress intended SCA warrants to apply extraterritorially, it would provide for such far-reaching state court authority without at least addressing the subject of conflicts with foreign laws and procedures.") (internal marks and quotations omitted).

[33] *Id.* at 217 ([T]he relevant provisions of the SCA focus on protecting the privacy of the content of a user's stored electronic communications. Although the SCA also prescribes methods under which the government may obtain access to that content for law enforcement purposes, it does so in the context of a primary emphasis on protecting user content.").

[34] *Microsoft*, 829 F.3d at 231 (Lynch, J., concurring) (emphasis in original).

[35] *Id.* at 222.

In this case, the government went through the most privacy-protective requirements in the SCA: obtaining a warrant for the content of communications in compliance with requirements established by the Fourth Amendment.[36] While the SCA, and ECPA broadly, may be ill-equipped to address the nuances of modern technology,[37] the privacy violations asserted by Microsoft and amici are not as grave as suggested.

While concurring in the court's holding, Judge Lynch further emphasized the serious need for Congress to revise the SCA to reflect current realities of stored electronic communications.[38] If, as the majority suggests, an invasion of privacy occurs where particular content is stored,[39] any future litigation against the government regarding information stored in the cloud will necessarily involve fact-dependent analyses of where information may have been at a particular moment it was searched or seized. A more appropriate solution may be to tie the "location" of the privacy invasion to the nationality or residence of the individual whose privacy was violated, rather than to the arbitrary and transitory location of the individual's data. However, doing so likely requires an amendment to the law, and would require Congressional attention.

LIKELY EFFECTS OF THE DECISION

In the wake of the *Microsoft* decision, commentators,[40] Congress,[41] and Microsoft itself[42] have noted the limitations of the SCA and ECPA as they currently stand. Many commentators, including Microsoft, hailed the Second

---

[36] *Id.*

[37] See Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1214 (2004) ("[T]here are many problems of Internet privacy that the SCA does not address.").

[38] *Id.* at 231-33. *See also* Peter J. Henning, *Microsoft Case Shows the Limits of a Data Privacy Law*, N.Y. TIMES (July 18, 2016), http://www.nytimes.com/2016/07/19/business/dealbook/microsoft-case-shows-the-limits-of-a-data-privacy-law.html.

[39] *See Microsoft*, 829 F.3d at 209; *id.* at 230 n.7. (Lynch, J., concurring).

[40] Andrew Keane Woods, *Reactions to the Microsoft Warrant Case*, LAWFARE BLOG (July 15, 2016, 7:21 AM), https://lawfareblog.com/reactions-microsoft-warrant-case.

[41] Press Release, Office of Senator Orrin Hatch, Orrin Hatch, Hatch, Coons, Heller Introduce Bipartisan International Communications Privacy Act, (May 25, 2016), http://www.hatch.senate.gov/public/index.cfm/2016/5/hatch-coons-heller-introduce-bipartisan-international-communications-privacy-act.

[42] Brad Smith, *Our Search Warrant Case: An Important Decision for People Everywhere*, MICROSOFT (July 14, 2016), http://blogs.microsoft.com/on-the-issues/2016/07/14/search-warrant-case-important-decision-people-everywhere/.

Circuit's decision as a victory for individual privacy.[43] This understanding of *Microsoft*'s outcome is largely flawed— while the majority opinion cited protecting individual privacy for users of cloud-based services as a motivation for its holding, the opinion missed important implications for individual privacy, as noted throughout Judge Lynch's concurrence.[44] Further diminishing the privacy issues cited by the majority, Microsoft did not contest that if all the data requested was stored in the United States, it would have provided content access to law enforcement.[45] Currently, the majority of such email data remains stored in the United States,[46] and as such, the effects of *Microsoft* are likely to remain limited in actual application in the near future.

A purely territorial approach to a user's privacy expectations (and to the SCA) is becoming increasingly challenging to manage judicially, as users are relying more frequently on cloud-based products and services, and companies providing cloud services continue to diversify the geographic scope of their servers.[47]

However, the localization of data poses complications beyond the scope encountered in *Microsoft*. The debate over the ability for data to actually be localized at all has not yet been settled: some argue that data, like money or debt, can indeed be localized,[48] while others note that such analogies to other forms of "intangible" items do not properly capture the way that data is stored and moved.[49]

This debate will certainly continue as the use of cloud storage expands. But discussions on data processing cannot be solely domestic: foreign law and international agreements play a large role. China has strict rules on the export of data;[50] U.S.-EU agreements on data privacy could have a major effect on

---

[43] *See id.*

[44] *Microsoft*, 829 F.3d at 233 (Lynch, J., concurring) ("without any illusion that the result should even be regarded as a rational policy outcome, let alone celebrated as a milestone in protecting privacy.").

[45] *Id.* at 223.

[46] *Where is My Data?*, MICROSOFT ONLINE SERVS., https://www.microsoft.com/online/legal/v2/?docid=25 (last visited Oct. 21, 2016).

[47] *Microsoft*, 829 F.3d at 50, n.7 (Lynch, J., concurring).

[48] Kevin Dockery, *Data Localization Takes Off as Regulation Uncertainty Continues*, WALL ST. J.: RISK AND COMPLIANCE BLOG (June 6, 2016 1:08 PM ET), http://blogs.wsj.com/riskandcompliance/2016/06/06/data-localization-takes-off-as-regulation-uncertainty-continues/.

[49] *See* Woods, *Against Data Exceptionalism*, *supra* note 23 at 1.

[50] *Data Transfers Out of China: What You Have to Consider Before You Press "Send,"* FRESHFIELDS BRUCKHAUS DERINGER, http://www.freshfields.com/en/global/Digital/data_transfer/?LangType=2057 (last visited Oct. 21, 2016).

access to various types of data,[51] regardless of their localization; and the implications of the EU's General Data Protection Regulation are so far unclear.[52] Any lasting solution for the storage of, and government access to, personal data will need to take place in legislatures, and in international negotiations.

Currently, law enforcement's access to data stored abroad is governed by the Mutual Legal Assistance Treaty (MLAT) process, by which countries negotiate rules for requesting and granting access for criminal investigations.[53] Because ECPA requires that any government entity seeking to compel data must attain a U.S. warrant, foreign governments flood the Department of Justice with MLAT requests.[54] The decision in *Microsoft* is the mirror of that: U.S. law enforcement may not access data stored abroad without seeking assistance from the affected foreign government. While there have been competing suggestions on how best to reform the MLAT process,[55] reform of ECPA itself is likely necessary to allow law enforcement to effectively access data while still protecting consumer privacy. Regardless of how reform is achieved, data localization will likely remain a result of company policy, rather than a

---

[51] *See* U.S. DEP'T OF COMM., EU-U.S. PRIVACY SHIELD FRAMEWORK PRINCIPLES (2016). The exact nature of these agreements is not yet clear, but they would theoretically allow foreign governments to serve warrants on U.S. technology companies and vice versa, eliminating the type of warrant limitations faced in *Microsoft* as well as the sometimes lengthy mutual legal assistance treaty (MLAT) request process. *See also* Devlin Barrett & Jay Greene, *U.S. to Allow Foreigners to Serve Warrants on U.S. Internet Firms*, WALL ST. J. (July 15, 2016 8:00 PM ET), http://www.wsj.com/articles/obama-administration-negotiating-international-data-sharing-agreements-1468619305.

[52] Dockery, *Data Localization Takes Off*, *supra* note 48.

[53] T. Markus Funk, *Mutual Legal Assistance Treaties and Letters Rogatory: A Guide for Judges*, FED. JUD. CTR. (2014), http://www.fjc.gov/public/pdf.nsf/lookup/mlat-lr-guide-funk-fjc-2014.pdf/$file/mlat-lr-guide-funk-fjc-2014.pdf.

[54] Andrew Keane Woods, *Procedural Options for Improving Cross-Border Requests for Data*, LAWFARE BLOG (Oct. 13, 2015, 7:58 AM), https://www.lawfareblog.com/procedural-options-improving-cross-border-requests-data.

[55] *Compare* Letter from Peter J. Kadzik, Assistant Attorney Gen., to Joseph R. Biden, President of the United States Senate (July 15, 2015) (conveying proposed legislation and a section-by-section analysis), http://www.netcaucus.org/wp-content/uploads/2016-7-15-US-UK-Legislative-Proposal-to-Hill.pdf. (proposing allowing select foreign governments to make requests for data under their own domestic standards), *with* Jennifer Daskal & Andrew K. Woods, *Cross-Border Data Requests: A Proposed Framework*, JUST SECURITY (Nov. 24, 2015, 8:03 AM), https://www.justsecurity.org/27857/cross-border-data-requests-proposed-framework/ (proposing that foreign governments be allowed access to data under certain restrictions only when "(i) the requesting government has a legitimate interest in the criminal activity being investigated; (ii) the target is located outside the United States; and (iii) the target is not a US person.").

regulatory or consumer choice.[56] Each internet service provider (ISP) still principally acts according to internal policies when granting or denying government requests for account information, including warrant requests. As such, this poses the risk that private companies will continue to determine data privacy policy, rather than the government.[57] Whether or not technology companies shift servers abroad to deliberately frustrate legitimate law enforcement prerogatives is irrelevant; if servers are shifted abroad simply to suit a perception of market expectations and possible legal risk, the result will be the same. Legitimate warrants for evidence pertaining to U.S. suspects will be rendered toothless, an unlikely intent of the drafters of the SCA, or the constituents they serve. Individual privacy must be protected, but will be better served, and result in fewer unintended consequences, by an approach that builds those protections on a more accurate factual foundation. Due to the variety of requests from government agencies, differing internal policies, and the limited resources of the offices granting warrants and processing requests, it would greatly benefit the government, the public, and ultimately the technology sector to focus future legislation on standardizing data requests and responses across the industry.

CONCLUSION

In the wake of the *Microsoft* decision, the U.S. Congress has contemplated numerous reforms to ECPA that would variously address the scope of the 2703 warrant[58] and expand U.S. law enforcement's access to data overseas.[59] In the meantime, consumers are left with a confusing patchwork of statutory obligations, common law, and private corporate policies that reduce overall protection for consumer privacy. As the issue is considered further both in the courts and in the legislature, a keen eye towards the actual technological underpinnings of user communications is essential in order to balance the need for effective law enforcement with the responsibility to protect individual privacy rights.

---

[56] Peter J. Henning, *Microsoft Case Shows the Limits of a Data Privacy Law*, N.Y. TIMES (July 18, 2016), http://www.nytimes.com/2016/07/19/business/dealbook/microsoft-case-shows-the-limits-of-a-data-privacy-law.html?_r=0.

[57] *Microsoft*, 829 F.3d 197, 224 (2d Cir. 2016).

[58] Electronic Communications Privacy Act Amendments Act of 2015, S. 346, 114th Cong. § 2 (2015); Email Privacy Act, H.R. 699, 114th Cong. § 2 (2015).

[59] International Communications Privacy Act, S. 2986, 114th Cong. § 2 (2016).