In re Search Warrant No. 16-960-M-1 to Google: Point of Disclosure Means Trouble for Companies Storing Data Overseas

I. Overview of the Case

The Federal Bureau of Investigations (FBI) served Google with two search warrants issued under probable cause per section 2703 of the Stored Communications Act (SCA) in August 2016.[1] The warrants ordered Google to disclose information associated with four Google accounts concerning two domestic wire fraud investigations. Both Google accounts belong to United States citizens.[2] While Google's headquarters is in the United States (US), it stores user data across its global data storage network.[3] Additionally, Google breaks apart the stored files into pieces and automatically moves them across its global network at any given point in time to optimize network performance.[4] Google complied with the search warrants to the extent that it turned over the requested information that it knew was located in the US.[5] Because the rest of the sought data was stored overseas and possibly in multiple countries, Google contested that it did not have to comply to the full extent of the search warrants.[6]

Consolidating the two search warrant cases, The United States Magistrate Judge for the Eastern District of Pennsylvania first addressed Google's challenge to the search warrants.[7] Following the Second Circuit Court of Appeals decision in In re a Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., Google argued that it did not have

---

[1] In re Search Warrant No. 16-960-M-01 to Google and In re Search Warrant No. 16-1061-M to Google, No. 16-960, 2017 WL 3535037, at *1-2 (E.D. Pa. Aug. 8, 2017) [hereinafter Google II]; see also 18 U.S.C. § 2703 (stating the requirements for the issuance of a warrant under the SCA).
[2] Id. at *1.
[3] Id.
[4] Id.
[5] Id. at *2.
[6] Id.
[7] See In re Search Warrant No. 16-960-M-01 to Google and In re Search Warrant No. 16-1061-M to Google, 232 F. Supp. 3d. 708, 708 (E.D. Pa. 2017) [hereinafter Google I].

to comply with the warrants because the requested data was stored outside of the United States and doing so was an extraterritorial application of the SCA.[8] The argued extraterritorial application of a statute implies that the statute seeks to regulate the conduct of persons that occur outside of the US.[9] However, the Magistrate Judge held that the user data request was a domestic application of the SCA because Google's headquarters is in California, Google's employees accessing the requested data and complying with the warrant are in California, and the FBI's agents reviewing the data are in Pennsylvania.[10] Hence, all of the activity related to the requested user data would occur in the US despite the fact that the requested data is stored internationally.[11] Google sought review of the Magistrate Judge's decision.[12] On review, the United States District Court for the Eastern District of Pennsylvania held that the magistrate judge did not err in his decision because all points of disclosure of the requested data occurred in the US and the information was never disclosed abroad despite being stored abroad.[13] Therefore, the FBI's warrant was a permissible domestic application of the SCA. In re Search Warrant No. 16-960-M-01 to Google and In re Search Warrant No. 16-1061-M to Google, No. 16-960, 2017 WL 3535037, at *10-11 (E.D. Pa. Aug. 8, 2017).

II. Background

[8] Id. at 710; see also In re a Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 829 F.3d 197, 222 (2nd Cir. 2016) [hereinafter Microsoft] (holding that a SCA warrant cannot lawfully compel a US based service provider to disclose user data store overseas to the government).
[9] Kenneth S. Gallant, What Exactly is "Extraterritorial Application" of a Statute, JURIST (May 28, 2013, 9:00 AM), http://www.jurist.org/forum/2013/05/kenneth-gallant-extraterritorial-application.php.
[10] Google I, 232 F. Supp. 3d. at 721.
[11] Id.
[12] Google II, 2017 WL 3535037, at *1.
[13] Id. at *10-11.

The SCA, passed as part of the Electronic Communications Privacy Act of 1986, regulates the interactions between government investigators and service providers through privacy protections that resemble the Fourth Amendment privacy protections.[14] The Fourth Amendment protects an individual's reasonable expectation of privacy.[15] Traditional forms of technology, like home computers, are separately protected by the Fourth Amendment; however, traditional legal means do not protect other aspects of computer networks.[16] The SCA fills in the gaps of privacy protection applied to the digital world in two ways: (1) it prevents the voluntary disclosure of electronic communication to the public; and (2) it sets the framework that the government must abide by to compel disclosure of such communications.[17] The privacy protections covered in the SCA apply to users of electronic communication services (ECS) and remote computing services (RCS).[18] An ECS gives users access to a central computer system to receive electronic communications.[19] An RCS gives users access to the computer processing facilities or by directly processing the transmitted data for a user and then transmitting back the requested results.[20] The creation of the two designations was in recognition that service providers could be acting as an ECS or an RCS or both and the scope of privacy protections needed to be tailored appropriately.[21] For example, when a user sends an email using their Gmail account, Google is acting as an ECS until the user reads the email.[22] If the user saves that email or simply

[14] 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, 1212 (2004).
[15] Id.
[16] Id. at 1214.
[17] Id. at 1212-13.
[18] Id. at 1214.
[19] 18 U.S.C. §2510(15).
[20] 18 U.S.C. § 2711(2).
[21] Id. at 1215-16.
[22] See id. at 1216.

leaves it in their inbox after reading it, Google is now acting as an RCS.[23] Because of the fluidity, the Act protects both services while Fourth Amendment privacy protections still apply to service providers that are not an ECS or an RCS.[24]

The protections outlined in the SCA are meant to limit the government's ability to compel service providers to disclose private user information without going through the proper legal processes.[25] Sections 2701, 2702, and 2703 are the main provisions of the SCA.[26] Section 2701 prohibits third parties from unauthorized access to stored communication, but it does not prevent a service provider from accessing the information stored on its network.[27] The SCA defines stored communications as "(a) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (b) any storage of such communication by an electronic communication service for purposes of backup protection of such communication."[28] Section 2702 bars service providers from purposefully disclosing the stored information and other user data, except by explicit permission or under Section 2703.[29] Section 2703 of the SCA establishes three ways in which the government may compel a service provider to disclose user information: a warrant, a court order, and an administrative subpoena.[30] For communications content like emails or documents stored in the cloud, the government must meet a higher standard by obtaining a search warrant issued by a judge under the Federal Rules of Criminal Procedure.[31] Additionally, if the government obtains a warrant, it is not required to

[23] Id.
[24] Id. at 1216-17.
[25] See id. at 1212-13.
[26] Google II, 2017 WL 3535037, at *3.
[27] 18 U.S.C. § 2701.
[28] 18 U.S.C. § 2510(17).
[29] 18 U.S.C. § 2702(b).
[30] 18 U.S.C. § 2703(b).
[31] 18 U.S.C. § 2703(a).

notify the user that the government has obtained a warrant to compel disclosure of their information from their service provider.[32]

As US-based technology companies have grown in international size that was unfathomable to drafters of the earlier legislation, the need to extend statutes extraterritorially to maintain the statute's focus has created a complex issue.[33] When analyzing extraterritoriality issues, meaning whether or not the government has the legal ability to extend its authority beyond the US borders, the Supreme Court has put forward a two-step framework. [34] In the first step of the framework, the court asks, whether there is an indication that the statute has an extraterritorial application.[35] If the statute does not rebut the presumption against extraterritorial application, then the court must address the second step of the analysis.[36] In the second step, the court postulates whether the case requires extraterritorial application in light of the statute's focus.[37] In other words, if the relevant conduct occurs in the US, it is a permissible domestic application of the statute regardless of the location of the other conduct.[38] If "the conduct relevant to the focus occurred in a foreign country, then the case involves an impermissible extraterritorial application regardless of any other conduct that occurred in U.S. territory."[39]

In Microsoft, the Second Circuit Court applied this two-step analysis and determined that the SCA does not apply to electronic communications stored overseas.[40] Addressing the first step of

---

[32] 18 U.S.C. § 2703(b)(1)(A).
[33] See Microsoft, 829 F.3d at 226.
[34] RJR Nabisco, Inc. v. European Cmty., 136 S. Ct. 2090, 2101 (2016); see also Morrison v. Nat'l Austl. Bank Ltd., 561 U.S. 247, 255 (2010) (holding that the default presumption of a federal law is against having an extraterritorial effect).
[35] RJR Nabisco, 136 S. Ct. 2090, 2101 (2016).
[36] Id.
[37] Id.
[38] Id.
[39] Id.
[40] Microsoft, 829 F.3d at 221-22.

the analysis, the Second Circuit analyzed whether the SCA discussed extraterritorial issues despite the fact that the government conceded that the SCA did not discuss extraterritorial issues at oral argument.[41] For a statute to apply extraterritorially, Congress must give an "affirmative indication" of the intent for a law to apply extraterritorially.[42] Without a clear sign giving the statute an extraterritorial reach, the presumption is against implementing a statute extraterritorially.[43] The court could not find text, structure, purpose, or legislative history showing Congress's implicit or explicit intent for the statute to apply extraterritorially.[44] Thus, the presumption is against extraterritorial application.[45]

Additionally, the Second Circuit addressed the second step of the analysis declaring that the SCA's focus was on the need to protect user's privacy interests in the electronic communications even if the relevant conduct occurs domestically.[46] The statute prohibits service providers from disclosing the stored communications unless an exception exists.[47] Accordingly, the government argued that the SCA warrant provisions shifted the focus of the statute to the point of disclosure rather than the privacy of the stored communications.[48] The SCA specifically uses the term "warrant" and adopts the Federal Rules of Criminal Procedure for obtaining warrants.[49] Using the term "warrant" implies a focus on protecting one against an invasion of privacy. Here, the court stated that "the invasion of the customer's privacy takes place under the SCA where the customer's protected content is accessed - here where it is seized by Microsoft, acting as an

[41] Id. at 210-11.
[42] Morrison, 561 U.S. at 265.
[43] Id.
[44] Microsoft, 829 F.3d at 203.
[45] Id.
[46] Id. at 218.
[47] Id.
[48] Id.
[49] Id.

agent of the government," at a data center in Ireland.[50] Therefore, the Court interpreted the term "warrant" in the SCA to provide increased privacy protection domestically because of the specific usage of the Federal Rules of Criminal Procedure rules that apply to purely domestic warrants as well.[51]

Further, the Second Circuit chose to respect the interests of other nations' laws that regulate cross-border criminal investigations.[52] The current process for governments to acquire overseas data related to ongoing criminal investigations is governed by Mutual Legal Assistance Treaties (MLATs).[53] Microsoft did disclose that the relevant user data was being stored on a single server in Ireland.[54] While the Court noted that MLATs are onerous and impede law enforcement efforts, Ireland is a signatory to the treaty, which makes MLAT the provision that governs the government's request for data stored overseas.[55] Therefore, the Court determined that the SCA does not require companies to produce documents stored overseas because the government's use of the SCA warrant would be incompatible with the presumption against extraterritoriality absent clear Congressional intent that the Supreme Court has previously emphasized in Morrison v. Nat'l Austl. Bank Ltd. and RJR Nabisco, Inc. v. European Cmty.[56]

In a concurring only in the judgment opinion, Judge Gerard Lynch focused on the changing nature of electronic communications and the location of that stored data.[57] He noted that the

---

[50] Id. at 218.
[51] Id.
[52] Id. at 221.
[53] Id.
[54] Id. at 220.
[55] Id. at 221.
[56] Id. at 222; see also RJR Nabisco, 136 S. Ct. at 2100 (holding that the presumption of a statute is against extraterritoriality absent congressional intent as federal laws are meant to apply only domestically); see also Morrison, 561 U.S. at 265 (concluding that the presumption against extraterritoriality requires a clear indication that the statute is meant to apply abroad).
[57] Microsoft, 829 F.3d at 224 (concurring Lynch, G., concurring).

location of the data was virtual.[58] Employees of the company could access the same data in the ordinary course of business without leaving their desks in the US or concerning themselves with the storage location.[59] Consequently, focusing on the location of the data is unnecessary because the conduct relevant to the information disclosure takes place domestically.[60]

III. Court's Decision

In the noted case, the United States District Court for the Eastern District of Pennsylvania affirmed Magistrate Judge Reuter's decision to grant the government's motion to compel Google to comply with the SCA search warrants.[61] The Court held that the point of disclosure of the requested information being in the US is a domestic application of the SCA regardless of the data's storage location.[62] Similar to Microsoft, the first step of the two-step analysis was undisputed.[63] Google and the government were in agreement that Section 2703 does not provide Congressional intent to apply the provision extraterritorially.[64] Accordingly, the heart of the case lies in the second step of the analysis, whether identifying the SCA's focus and the relevant conduct to the SCA's focus includes a domestic application of the statute.[65]

The Court agreed with the government that the SCA warrant was not a traditional search warrant.[66] While a traditional search warrant is issued based on a certain place, an SCA warrant is directed to the service provider.[67] The government's argument hinges on this distinction

---

[58] Id. at 229.
[59] Id.
[60] Id.
[61] Google II, 2017 WL 3535037, at *11.
[62] Id. at *10-11.
[63] Id. at *6; see also Microsoft, 829 F.3d at 210 (concluding that Congress did not intend Section 2703 to have an extraterritorial application).
[64] Google II, 2017 WL 3535037, at *6.
[65] Id.
[66] Id. at *7.
[67] Id.

between place and person that the warrant may be enforced to search the information in the service providers control, regardless of location.[68] Google argued that the use of the term "warrant" was Congress' intent to mean an authorization to search and seize private property located in the US within the territorial reach of the warrant.[69] However, the court concluded that the SCA warrant is a mechanism that the government uses to compel a service provider to disclose electronic communication information in its possession rather than tied to a location.[70] In practice, the warrant is more characteristic of other forms of legal processes analogous to a subpoena or court-ordered discovery that reach information in the control of the party that the particular court has personal jurisdiction over.[71] In deciding that the SCA warrant provision is a hybrid of other legal forms, the Court had to also decide on what activity the provision seeks to regulate and where that activity ultimately takes place.[72]

Applying this analysis, the Court decided that the conduct the SCA sought to regulate was the disclosure of the information to the government, which would solely occur in the US.[73] While Section 2702 prohibits a provider from disclosing user information to third parties, Section 2703 outlines exceptions to this rule.[74] Rather than a focus on enhanced privacy as Google argues, compelled disclosure and the conduct related to the disclosure is the focus of the statute. Under the SCA, Google can move its user's data, and Google's storage practices indicate that it moves its user's data constantly.[75] The statute solely prevents Google from disclosing the

[68] Id.
[69] Id. at *6
[70] Id. at *7.
[71] Id.
[72] Id. at *7-8.
[73] Id. at *8
[74] Id. at *10; see also 18 U.S.C. § 2703 (detailing the specific disclosure exceptions).
[75] Id. at *10

data to the government absent a warrant.[76] Thus, the Court concluded that enforcing the warrant was a domestic application of the SCA because it was issued in the US to a US-based service provider and required disclosure in the US.[77]

Additionally, the Court addressed Google's argument that the conduct relevant to gathering the requested data stored overseas occurred largely outside of the US. As part of Google's network efficiency storage practices. Google automatically moves and breaks apart the data between its data centers to optimize its network performance, reliability, and efficiency.[78] Thus, Google asserted that the querying for the requested data would run on servers in Google's foreign data centers.[79] Consequently, the Court found, even still, that the conduct relevant to the targeted data occurred in the US.[80] The difficulty of physically locating the data on Google's systems favored the warrants reaching beyond the US.[81] By Google's assertions, it designates a team of employees based in California to comply with data requests under the numerous government warrants that the company receives.[82] This dedicated team means that Google's headquarters is the only place used to access the data.[83] As the data requested is lawfully accessed, disclosed, and transferred in the US according to the warrant, Google was required to comply with the government's SCA warrants.[84]

IV. Analysis

---

[76] Id.
[77] Id.
[78] Id.
[79] Id.
[80] Id.
[81] Id.
[82] Id. at *2.
[83] Id.
[84] Id. at *11

The Eastern District of Pennsylvania Court correctly held, based on the focus of Section 2703, that compliance with the search warrant was not an extraterritorial application of the SCA.[85] Section 2703 focuses on how the government may compel a service provider to disclose information under a warrant issued under probable cause.[86] The dispute is not about Section 2703's concentration on disclosure.[87] The argument is regarding where that disclosure is taking place.[88] Under the government's construction of the argument, Section 2703 is the only relevant section of the statute authorizing the government to compel disclosures of information in the US.[89] Based on Section 2702, this argument appears to have merit as the service providers are allowed to move information across its network.[90] Based on the plain text, the Court focused on the location of the service provider as the fixed location of the data regardless of the service's provider's ability to move data throughout its network.[91] The argument, while textually correct, highlights the outdatedness of the SCA as it has become bureaucratic and sets unclear practices for large-scale, multinational technology companies to follow.[92] Even though the court is cautious in abiding by the plain text of the statute, the attempt to apply US law to conduct abroad can cause unforeseen tension with those countries.

---

[85] See id. at *11
[86] See 18 U.S.C. § 2703.
[87] See Google II, 2017 WL 3535037, at *10; see also Microsoft, 829 F.3d at 228 (Lynch, J., concurring) (noting that the SCA reaches records in control of a party of which the court has personal jurisdiction over).
[88] See Google II, 2017 WL 3535037, at *9.
[89] See id.
[90] See 18 U.S.C. § 2702; see also Google II, 2017 WL 3535037, at *9 (noting that Section 2703 creates exceptions to Section 2702's default prohibition against data disclosures to third parties).
[91] See Google II, 2017 WL 3535037, at *10.
[92] See Tess Townsend, Google has Proposed Changes in Laws Requesting Data, RECODE (Jun. 22, 2017, 2:36 PM), http://www.recode.net/2017/6/22/15855322/google-change-laws-access-user-data-international.

In recognition of the international dichotomy at play, the Court validly distinguished the case from Microsoft.[93] The Microsoft decision left an option for the government to use the existing Mutual Legal Assistance Treaty (MLAT) channels to compel disclosure of the sought data.[94] Despite the slow MLAT process especially for time-sensitive investigations, the Second Circuit acknowledged that MLAT was a substitute for Section 2703 warrants.[95] However, MLAT would not be a reliable substitute for the government based on Google's automated storage practices.[96] While Microsoft was able to isolate the location of the requested data to a single server in Ireland and agreed to keep it there for a MLAT request, Google claims that it does not know the location of a single piece of data at any given point.[97] If Google's claims were accepted, the government would never be able to compel disclosure of stored communications for its ongoing criminal investigation. Therefore, the Court focused on Google's domestic and centralized headquarters in the US as the easier location to state as the location of information disclosure and as a way facilitate the government's ability to investigate criminal activity promptly.[98]

Despite a textually sound argument and a distinguishable set of facts from Microsoft, the Court sets a dangerous precedent.[99] In effect, the Court stated that US warrants could reach anywhere in the world provided the warrant is served to a service provider's domestic offices

---

[93] See Google II, 2017 WL 3535037, at *5; see also Microsoft, 829 F.3d at 220-21 (concluding that the conduct relevant to the SCA's focus would occur in Microsoft's Ireland data center).
[94] See Microsoft, 829 F.3d at 221.
[95] See id.
[96] See In re Search of Information Associated with [redacted]@gmail.com that is Stored at Premises Controlled by Google, Inc., No. 16-mj-757, 2017 WL 3445634, at *26-27 (D.D.C. July 31, 2017) (noting that the Microsoft decision is counter to established law but also fails to protect customer privacy).
[97] See Google II, 2017 WL 3535037, at *5.
[98] See id. at *10-11.
[99] See John P. Carlin and Joseph Roth Rosner, Google Ordered to Comply with Warrant for Foreign-Stored User Data, MORRISON FORRESTER (Feb. 13, 2017), http://www.mofo.com/resources/publications/170210-google-ordered-to-comply.html.

and the compiling of the data for the warrant occurs in the US.[100] The government also shows that it continues to press the same arguments it raised in Microsoft and accentuates the fact that the Second Circuit's decision is an anomaly.[101] While the court focused on determining the focus of the statute, the issue in these cases is the statute itself.[102] The Supreme Court has unequivocally held that there is a presumption against the extraterritorial application of a statute absent clear congressional intent.[103] Adopted in 1986, the SCA was written with the mindset that US service providers would store US customer's data on US servers in US data centers.[104] The notion of an extraterritorial application was not considered because technological advancements like global cloud computing were not in practice.[105] Thus, the issue lies with Congress and the need to update an out-of-date law, not the debate between the statute's focus as either on disclosure or privacy.[106] As a consequence, companies must now re-evaluate its storage practices as these legal developments are being handed down.[107]

---

[100] See Letter from Apple et al., to Senators Hatch, Coons, and Heller (Aug. 1, 2017) (on file with Senator Hatch).
[101] See Carlin and Rosner, supra note 99.
[102] See Orin Kerr, Google Must Turn Over Foreign-Stored Emails Pursuant to a Warrant, Court Rules, THE WASHINGTON POST (Feb. 3, 2017), http://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/02/03/google-must-turn-over-foreign-stored-e-mails-pursuant-to-a-warrant-court-rules/?utm_term=.ff53bd003584.
[103] See RJR Nabisco, 136 S. Ct. at 2100; see also Morrison, 561 U.S. at 265 (concluding clear Congressional intent to apply a statute abroad is needed to rebut the presumption against extraterritoriality).
[104] See Orin Kerr, What Legal Protections Apply to E-mail Stored Outside the U.S., THE WASHINGTON POST (July 7, 2014), http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/07/07/what-legal-protections-apply-to-e-mail-stored-outside-the-u-s/?tid=a_inl&utm_term=.3438222b3a92
[105] See Microsoft, 829 F.3d at 231 (Lynch, G., concurring).
[106] See Kerr, supra note 102.
[107] See id.

Given the number of cases challenging the extraterritoriality of the SCA, the issue has become contentious.[108] Unfortunately for Google and other service providers storing data overseas, courts in five different districts continue to reject the Second Circuit's decision in Microsoft.[109] Since a number of rulings against Google have come out, it is highly unlikely that the decisions will be reversed on appeal.[110] The growing trend is that the location of the service provider or the location where the retrieval of the data will take place is more important than where the companies store the data.[111] The trend, though, causes further disruption in the ability for companies to implement cross-border data transfers, as US service providers may experience more difficulties from foreign governments that understand the government's search warrants to now have a global reach.[112] Companies see this sentiment primarily in Europe following the European Court of Justice's 2015 decision to strike down the long-standing safe harbor data

---

[108] Justine Brown, Judge Says Google Must Comply with Email Search Warrant, CIO DIVE (Feb. 6, 2017), http://www.ciodive.com/news/judge-says-google-must-comply-with-email-search-warrant/435512/.

[109] See In re Search Warrant to Google, Inc., No. 17-mj-532 (N.D. Ala. Sept. 1, 2017), slip op. 23; In re Search Warrant No. 16-960-M-1 to Google, No. 16-960, 2017 WL 3535037, at *11 (E.D. Pa. Aug. 17, 2017), aff'g 232 F. Supp. 3d 708 (E.D. Pa. Feb. 3, 2017); In re Search of Content Stored at Premises Controlled by Google Inc., No. 16-mc-80263, 2017 WL 3478809, at *5 (N.D. Cal. Aug. 14, 2017), aff'g 2017 WL 1487625 (N.D. Cal. Apr. 25, 2017); In re Search of Information Associated with [redacted]@gmail.com that is Stored at Premises Controlled by Google, Inc., No. 16-mj-757, 2017 WL 3445634, at *27 (D.D.C. July 31, 2017), aff'g 2017 WL 2480752 (D.D.C. June 2, 2017); In re Search of Information Associated with Accounts Identified as [redacted]@gmail.com, No. 16-mj-2197, 2017 WL 3263351, at *9 (C.D. Cal. July 13, 2017); In re Search Warrant to Google, Inc., No. 16-4116, 2017 WL 2985391, at *12 (D.N.J. July 10, 2017); In re Two Email Accounts Stored at Google, Inc., No. 17- M-1235, 2017 WL 2838156, at *4 (E.D. Wis. June 30, 2017); In re Search of Premises Located at [Redacted]@yahoo.com, No. 17-mj-1238 (M.D. Fla. Apr. 7, 2017), slip op. 3.

[110] Sophia Morris, Google Won't Challenge Warrants For Overseas Data: DOJ, LAW360 (Sept. 14, 2017, 6:04 PM), http://www.law360.com/articles/964048/google-won-t-challenge-warrants-for-overseas-data-doj.

[111] Id.

[112] See In re Search of Information Associated with [redacted]@gmail.com that is Stored at Premises Controlled by Google, Inc., 2017 WL 3445634 at *27.

transfer deal with the US.[113] The European Court's decision invalidated the agreement citing misuses of European citizen's personal data with no judicial means of redress in the US for these European citizens and concerns over US law enforcement having unrestrained access to the transferred data.[114] As a result, a new agreement, the EU-US Privacy Shield, was crafted out of this decision to continue the transfers of data between Europe and the US but with added policing mechanisms.[115] With the Google decision compelling the disclosure of data stored overseas being the predominant viewpoint of the US courts, the decision is playing into the exact fears that the European Union has laid out regarding the US government's reach.[116] Such legal uncertainty is setting the stage for profound implications for multinational corporations.[117] Because the Second Circuit's decision is still valid law in that circuit, the possibility of a Supreme Court decision to establish a uniform standard of implementing SCA warrants increases.[118]

Nevertheless, Google has mostly decided not to fight rulings outside of the Second Circuit.[119] Instead, Google has joined many fellow service providers in support of the International Communications Privacy Act (ICPA), a recently introduced bill in the Senate that seeks to modernize the legal process for law enforcement to request international data.[120] The companies

---

[113] See CJEU 6 October 2015, Case C-362/14, Schrems, ECLI:EU:C:2015:650.
[114] See id.
[115] See Allison Grande, What to Watch With EU-US Privacy Shield Under Microscope, LAW360 (Sept. 15, 2017, 9:31 PM), http://www.law360.com/articles/964150/what-to-watch-with-eu-us-privacy-shield-under-microscope.
[116] See id.
[117] See id.
[118] See Carlin and Rosner, supra note 99.
[119] See Reply Brief of Petitioner-Appellant at 9, United States v. Microsoft Corp., No. 17-2 (Sept. 13, 2017).
[120] See International Communications Privacy Act (ICPA), S. 2986, 114th Cong. (introduced May 16, 2016); see also Letter from Apple et al., supra note 88 (listing Google as one of the technology leaders in support of the ICPA).

and judges want to update this out-of-date statute to comply with multiple privacy laws and regulations as well as to assist law enforcement officers in their duties.[121] Until Congress enacts new legislation or the Supreme Court issues a definitive ruling, companies deciding how to respond to these warrants will hinder government investigations and perpetuate the legal ambiguity that surrounds overseas data storage.[122]

[121] See Ali Breland, Senate Bill Would Ease Law Enforcement Access to Overseas Data, THE HILL (Aug. 1, 2017 4:19 PM), http://thehill.com/policy/technology/344823-senators-introduce-new-bill-to-force-law-enforcement-to-obtain-americans; see also Microsoft, 829 F.3d at 224 (Lynch, G., concurring) (believing that the SCA should be revised despite agreeing with the majority's interpretation of the statute).

[122] Carlin and Rosner, supra note 99.