SUSAN L. CARNEY, *Circuit Judge*, concurring in the order denying rehearing *en banc*:

The original panel majority opinion, *see Microsoft Corp. v. United States*, 829 F.3d 197 (2d Cir. 2016), fully explains why quashing the government's warrant is called for by Supreme Court precedent on extraterritoriality and the text of the Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701 *et seq*. Because the panel opinions did not include a dissent, however, I write again, briefly, to respond with respect to several points raised during our Court's consideration of whether to grant the government's petition for *en banc* review and reflected in the dissents from denial of rehearing.[1]

The theme running through the government's petition and the dissents is the concern that, by virtue of the result the panel reached, U.S. law enforcement will less easily be able to access electronic data that a magistrate judge in the United States has determined is probably connected to criminal activity.[2] My

[1] Judges Lynch and Bolden, who comprised the rest of the panel that heard this appeal, are not eligible to participate in deciding whether to rehear this case *en banc* because they are, respectively, a judge who entered senior status not long before the *en banc* poll was requested and a district judge sitting by designation. *See* 28 U.S.C. § 46(c) (limiting *en banc* voting to "the circuit judges of the circuit who are in regular active service").

[2] In this regard, it bears noting that an SCA section not at issue in this case, 18 U.S.C. § 2702(b)(8), authorizes "[a] provider . . . [to] divulge the contents of a communication . . . to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person

panel colleagues and I readily acknowledge the gravity of this concern. But the SCA governs this case, and so we have applied it, looking to the statute's text and following the extraterritoriality analysis of *Morrison v. National Australia Bank Ltd.*, 561 U.S. 247 (2010). We recognize at the same time that in many ways the SCA has been left behind by technology. It is overdue for a congressional revision that would continue to protect privacy but would more effectively balance concerns of international comity with law enforcement needs and service provider obligations in the global context in which this case arose.[3]

Before going further, it is worth pointing out what is *not* at issue in this appeal. First, it is common ground that Congress did not intend for the SCA's warrant procedures to apply extraterritorially. *See* Gov't Pet. for Reh'g 11. Second, although the panel majority determined that the SCA's focus lies on protecting user privacy, this determination was made under the second part of

---

requires disclosure without delay of communications relating to the emergency," bypassing the warrant procedures of § 2703. Another section gives a provider immunity from civil liability for a voluntary production of content made "in accordance with . . . [a] statutory authorization . . . under this chapter." 18 U.S.C. § 2703(e). The panel expressed no opinion on the use of these subsections, nor has it been suggested that the exigent circumstances of a "danger of death or serious physical injury" are presented here.

[3] This is a fact well appreciated by the Members of Congress who have introduced a bill proposing related amendments. *See* International Communications Privacy Act, S. 2986, H.R. 5323, 114th Cong. (2016).

the extraterritoriality analysis set forth as a canon of construction in *Morrison* and recently developed further in *RJR Nabisco, Inc. v. European Community*, 136 S. Ct. 2090 (2016). *See RJR Nabisco*, 136 S. Ct. at 2101 ("If the statute is not extraterritorial, then at the second step we determine whether the case involves a domestic application of the statute, and we do this by looking to the statute's 'focus.'"). Our "focus" analysis did not turn on privacy protections independently derived from the Fourth Amendment. Nor did we express or imply a view about how Congress *may* permissibly legislate to enable the government to reach data stored abroad and under the control of U.S. companies; our reading of the SCA did no more than adhere to the dictates of *Morrison* in construing the SCA. Finally, since the instrument was issued by a neutral magistrate judge upon a showing of probable cause, no one disputes that the Microsoft warrant has satisfied the most stringent privacy protections our legal system affords.

Accordingly, the dispositive question in the case, as we see it, might be framed as whether Microsoft's execution of the warrant to retrieve a private customer's electronic data, stored on its servers in Ireland, would constitute an extraterritorial application of the SCA in light of the statute's "focus,"

determined in accordance with *Morrison* and *RJR Nabisco*. Again, this is a question of statutory construction. And, unsurprising in light of the need for an extraterritoriality analysis, it requires consideration of the concerns of sovereignty and international comity.

The panel majority concluded that "the relevant provisions of the SCA focus on protecting the privacy of the content of a user's stored electronic communications." *Microsoft*, 829 F.3d at 217. The concurring opinion noted the difficulty in determining a statute's "focus" under *Morrison*, but agreed that in the absence of any evidence that Congress intended the SCA to reach electronic data stored abroad by a service provider (and relating potentially to a foreign citizen), the effect of the government's demand here impermissibly fell beyond U.S. borders and therefore the Microsoft warrant should be quashed. *Id.* at 230-31 (Lynch, *J.*, concurring).

Guided by our determination of the statute's focus and looking at the text of the SCA itself, the panel majority read the statute to treat the locus of the SCA's privacy protections as at the place of data storage. As further detailed in the majority opinion, this conclusion comports with the SCA's reliance on the fact and form of content storage as predicates to its various provisions, as well as

its use of the term of art "warrant" and its requirement of compliance with Federal Rule of Criminal Procedure 41, "Search and Seizure"—features usually associated with physical access. *See, e.g.*, 18 U.S.C. § 2701(a) (prohibiting access to "facilit[ies]" where electronic communications are stored); *id.* § 2702(a)(1)-(2) (prohibiting disclosure of communications "while in electronic storage" or "which [are] carried or maintained" by an electronic communication service); *id.* § 2703(a) (imposing warrant procedures on electronic communications that are "in electronic storage in an electronic communications system for one hundred and eighty days or less"). We noted that the statute uses "[t]he circumstances in which the communications have been stored . . . as a proxy for the intensity of the user's privacy interests, dictating the stringency of the procedural protection they receive." *Microsoft*, 829 F.3d at 217. We also noted that § 2701, by proscribing unauthorized access to storage facilities, not only limits disclosure but also "shelters the communications' integrity." *Id.* at 218. Because the electronic communications to be accessed and disclosed pursuant to the Microsoft warrant are stored in a Dublin datacenter, we reasoned, the execution of the warrant would have its effect when the service provider accessed the data in Ireland, an extraterritorial application of the SCA.[4]

[4] This approach, in which we considered several numbered sections of the SCA, is not

Characterizing the statute's focus differently, as resting on "disclosure," and offering a detailed recitation of the available statutory support for that conclusion,[5] the dissents argue primarily that the SCA's effect occurs at the place

---

inconsistent with *RJR Nabisco*. Rather than requiring a provision-by-provision analysis in every instance, as the government and some of the dissenters suggest in the context of their "focus" analysis, *see post* at 2 (Droney, *J.*, dissenting from the denial of reh'g *en banc*), *RJR Nabisco* involved looking at the expressed congressional intent with regard to the separately-enacted RICO predicate statutes, one by one, in the context of an overarching structure—that is, RICO. The panel majority here saw the SCA's relevant provisions, essentially enacted of a piece, as reflecting a single congressional expression with respect to extraterritorial application—a statutory circumstance quite different from the one addressed in *RJR Nabisco*.

[5] In support of their position my dissenting colleagues contend, as does the government, that an SCA warrant functions more like a subpoena than a traditional warrant and should be treated accordingly as reaching all documents under the control of the instrument's recipient. *See post* at 7 n.19 (Cabranes, *J.*, dissenting from the denial of reh'g *en banc*); *id.* at 1 (Jacobs, *J.*, dissenting from the denial of reh'g *en banc*). The SCA does not address a potential extraterritorial application of the instrument issued under § 2703—indeed it is unlikely, in view of the historical context, that Congress could have anticipated such an application, much less weighed domestic law enforcement interests against countervailing concerns with international comity. In light of the importance of these interests, it seems a stretch to conclude that we should read Congress's deliberate choice of the term "warrant" to reflect a concurrent intention to incorporate into the statute, without explicit mention, a body of case law addressing not warrants, but grand jury subpoenas. *Cf. id.* at 7 n.19 (Cabranes, *J.*, dissenting from the denial of reh'g *en banc*) (citing *Marc Rich & Co. v. United States*, 707 F.2d 663 (2d Cir. 1983)). Even the territorial reach of subpoenas is not an easy determination, in light of the many interests that courts must balance when addressing discovery that has foreign aspects. *See, e.g.*, Restatement (Third) of the Foreign Relations Law of the United States § 442(1)(c) (listing several factors courts "should take into account" when deciding whether to order production of information located abroad). Some of my dissenting colleagues also emphasize that the customer data at issue here is already in Microsoft's possession. *See post* at 9-11 (Raggi, *J.*, dissenting from the denial of reh'g *en banc*). The SCA constrains a service provider's use of that "possession," recognizing the provider's role as an

of disclosure, on U.S. soil.[6] Thus, so long as (1) the warrant is served in the United States on a provider doing business in the United States, and (2) the provider can access the user's content electronically from the United States, extraterritoriality need not even be considered.[7] Since the warrant recipient here

---

intermediary between the customer who created the content and third parties. Thus, it distinguishes in its level of privacy protections between customers' substantive content and the administrative data that a provider maintains for its own purposes with respect to those customers. *See* 18 U.S.C. § 2703(c) (distinguishing between "contents of communications" and information such as a customer's name, address, and service details).

[6] As explored further below, although the SCA is broadly focused on privacy, it does address disclosure, most particularly in § 2702, as an exception to its general rule of maintaining the confidentiality of customer content. *See post* at 10-13 (Cabranes, *J.*, dissenting from the denial of reh'g *en banc*). The panel majority read the SCA to focus foremost on protecting user privacy by controlling access to stored communications—controls that apply even to service providers (if, for example, an employee exceeded his or her authorization with respect to stored data). To the extent that the majority opinion "raises concerns about the extraterritorial reach of *protections* from unlawful access and disclosures afforded by sections 2701 and 2702," *id.* at 14 n.36 (Cabranes, *J.*, dissenting from the denial of reh'g *en banc*) (emphasis added), one might take some comfort from the privacy laws of other countries that would apply to servers on their territory (and the significant incentives for service providers to guard against unauthorized intrusion). More importantly, however, the dissents' concerns about the reach outside the United States of the protections established by the statute provide yet another reason for congressional overhaul of the SCA.

[7] Taken to its logical conclusion, the dissents' focus on the place of disclosure to the exclusion of other factors would mean that, so long as the requested data is to be disclosed to the government within the United States, the SCA has only domestic application. But because, presumably, data demanded by the United States government under the SCA can *always* be expected to be disclosed to the government in the United States absent special circumstances, no application of the SCA's data disclosure procedures would be extraterritorial. At a time when U.S. companies, to their great

is Microsoft, a U.S. corporation (though the reasoning would apply equally well to a foreign provider who is sufficiently present in the United States), and the data is accessible and producible by Microsoft to the U.S. government in the United States, no more is needed to enforce the warrant. The inquiry stops there.

The panel majority rejected this position, and a few reflections illustrate why we were correct to do so. First: The position of the government and the dissenters necessarily ignores situations in which the effects outside the United States are less readily dismissed, whichever label is chosen to describe the "focus" of the statute. For example, under the dissents' reasoning (as we understand it), the SCA warrant is valid when (1) it is served in the United States on a branch office of an Irish service provider, (2) it seeks content stored in Ireland but accessible at the U.S. branch, (3) the account holding that content was opened and established in Ireland by an Irish citizen, (4) the disclosure demanded by the warrant would breach Irish law, and (5) U.S. law enforcement could request the content through the MLAT process.[8] This hardly seems like a

---

credit, provide electronic communications services to customers resident around the globe, this observation suggests the demerits of the analysis.

[8] As noted in the panel majority opinion, MLATs are Mutual Legal Assistance Treaties "between the United States and other countries, which allow signatory states to request one another's assistance with ongoing criminal investigations, including issuance and

"domestic application" of the SCA. Rather, we find it difficult to imagine that the Congress enacting the SCA envisioned such an application, much less that it would not constitute the type of extraterritorial application with which *Morrison* was concerned. Indeed, calling such an application "domestic" runs roughshod over the concerns that undergird the Supreme Court's strong presumption against extraterritoriality, and suggests the flaw in an approach to the SCA that considers only disclosure. *See Morrison*, 561 U.S. at 269 (citing "probability of incompatibility with applicable laws of other countries" as signaling absence of congressional attention to extraterritorial application); *EEOC v. Arabian Am. Oil Corp.*, 499 U.S. 244, 248 (1991) (observing that presumption against extraterritoriality "serves to protect against unintended clashes between our laws and those of other nations").

---

execution of search warrants." *Microsoft*, 829 F.3d at 221. The United States has entered into approximately 56 MLATs with foreign countries, including all member states of the European Union, and holds related Mutual Legal Assistance Agreements with others. *See id.* n.29; U.S. Dep't of State, *Treaties & Agreements*, https://www.state.gov/j/inl/rls/nrcrpt/2012/vol2/184110.htm. As the dissenters fairly point out, however, the United States lacks an MLAT relationship with many countries, and the MLAT process can be cumbersome. *See post* at 5 n.11 (Cabranes, *J.*, dissenting from the denial of reh'g *en banc*). In this case, the Republic of Ireland filed a brief *amicus curiae*, acknowledging its MLAT with the United States and representing its willingness "to consider, as expeditiously as possible, a request under the treaty." Br. *Amicus Curiae* Ireland 4, *Microsoft Corp. v. United States*, No. 14-2985 (2d Cir. December 2014).

Second: My dissenting colleagues take issue with the idea that "privacy" can have a territorial locus at all when it comes to electronic data, given the ease with which the data can be subdivided or moved across borders and our now familiar notion of data existing in the ephemeral "cloud." But, mundane as it may seem, even data subject to lightning recall has been stored somewhere, and the undisputed record here showed that the "somewhere" in this case is a datacenter firmly located on Irish soil.[9] *See Microsoft*, 829 F.3d at 220 n.28. (Fragmentation, an issue raised by the government in its petition and by the dissents here, was not present in the facts before the panel, and only further emphasizes the need for a modernized statute.) When Congress passed the "*Stored* Communications Act" in 1986, the statute it enacted protected data by limiting access to the "facility" where the data is stored or through which electronic services are provided. 18 U.S.C. § 2701(a). It did not address the

[9] Microsoft represents in the record that it stores data in different locations around the world not at whim, but for competitive commercial reasons: so that the data can be more quickly recalled for users based on proximity to their reported geographic locations. *See Microsoft*, 829 F.3d at 202. The record contains no basis for speculating that it has stored data in locations engineered to avoid an obligation to produce the data in response to law enforcement needs or to enable criminal activity to go undetected. Nor, although a customer could certainly do so, does the record suggest that the customer whose account is at issue falsely designated Ireland as its location to escape the reach of U.S. law enforcement. That customer could as well be a citizen of Ireland as of any other nation.

citizenship of the account holder, the nationality of the service provider, or any of the concerns that can be cited, legitimately, as relevant today to defining a sound policy concerning the privacy and disclosure of protected user content in a global setting. Nor have we been pointed to evidence suggesting that sovereigns have relinquished any claim to control over data physically stored within their boundaries. (Ireland certainly did not do so here in its submission *amicus curiae*.) Although the realities of electronic storage have widely outstripped what Congress envisioned in 1986, we are not so far from the context of the SCA that we can no longer apply it faithfully.

To connect these two points: Some of my dissenting colleagues, *see post* at 5 (Jacobs, *J.*, dissenting from the denial of reh'g *en banc*), like the panel, have noted potential concerns with reciprocity—that if the United States can direct a service provider with operations in the United States to access data of a foreign citizen stored in a foreign country, a foreign sovereign might claim authority to do the same and access data of a U.S. citizen stored in the United States, so long as the data would be disclosed abroad. If this concern holds any intuitive force, it does so only because the location of data storage *does* still have import, and therefore reaching across physical borders to access electronic data gives us pause when

we are on the receiving end of the intrusion. It is for just this sort of reason that the government has entered into MLATs with other sovereigns: to address mutual needs for law enforcement while respecting sovereign borders. And it is for just this sort of reason that the government has in other circumstances taken a position, somewhat in tension with the one it takes here, that courts should be particularly solicitous of sovereignty concerns when authorizing data to be collected in the United States but drawn from within the boundaries of a foreign nation. *See, e.g.*, Br. United States *Amicus Curiae* Opp'n Pet. Writ Cert. 8-21, *Arab Bank, PLC v. Linde*, No. 12-1485 (May 2014) (contending, in civil discovery context, that lower courts erred in "failing to accord sufficient weight to the foreign jurisdictions' interests in enforcing their bank secrecy laws").

Third, and finally: The exercise of selecting a "focus" and then determining its territorial locus highlights some of the difficulties inherent in applying the *Morrison* extraterritoriality analysis. Where the panel majority and the dissents diverge most sharply and meaningfully is on the better view of the legal consequences of the focus inquiry: *where*—for purposes of assessing extraterritoriality according to the Supreme Court's precedents—to locate the affected interest. Once we concluded that the statute focuses on protecting

privacy, the panel majority had to assess further where privacy might be considered to be physically based—an elusive inquiry, at best. As noted, the dissents emphasize disclosure, and reason from that premise that the place of disclosure establishes whether the proposed application of the statute is domestic. But we saw the overarching goal of the SCA as protecting privacy and allowing only certain exceptions, of which limited disclosure in response to a warrant is one. Considerations of privacy and disclosure cannot be divorced; they are two sides of the same coin. By looking past privacy and directly to disclosure, however, the dissents would move the "focus" of the statute to its exceptions, and away from its goal. The better approach, which in our estimation is more in keeping with the *Morrison* analysis and the SCA's emphasis on data storage, is one that looks to the step taken before disclosure—access—in determining privacy's territorial locus.

With a less anachronistic statute or with a more flexible armature for interpreting questions of a statute's extraterritoriality, we might well reach a result that better reconciles the interests of law enforcement, privacy, and international comity. In an analytic regime, for example, that invited a review of the totality of the relevant circumstances when assessing a statute's potential

extraterritorial impact, we might be entitled to consider the residency or citizenship of the client whose data is sought, the nationality and operations of the service provider, the storage practices and conditions on disclosure adopted by the provider, and other related factors. And we can expect that a statute designed afresh to address today's data realities would take an approach different from the SCA's, and would be cognizant of the mobility of data and the varying privacy regimes of concerned sovereigns, as well as the potentially conflicting obligations placed on global service providers like Microsoft. As noted above, there is no suggestion that Congress could not extend the SCA's warrant procedures to cover the situation presented here, if it so chose.

These were not the statutory context and precedent available to the panel, however, nor would they be available to our Court sitting *en banc*. Under the circumstances presented to us, the Microsoft warrant was properly quashed.