14-2985
Microsoft Corp. v. United States

United States Court of Appeals
FOR THE SECOND CIRCUIT

At a stated term of the United States Court of Appeals for the Second Circuit, held at the Thurgood Marshall United States Courthouse, 40 Foley Square, in the City of New York, on the 24th day of January, two thousand seventeen.

PRESENT: ROBERT A. KATZMANN,
Chief Judge,
DENNIS JACOBS,
JOSÉ A. CABRANES,
ROSEMARY S. POOLER,
REENA RAGGI,
PETER W. HALL,
DEBRA ANN LIVINGSTON,
DENNY CHIN,
RAYMOND J. LOHIER, JR.,
SUSAN L. CARNEY,
CHRISTOPHER F. DRONEY,
Circuit Judges.

- -x

In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation

- -x

MICROSOFT CORPORATION,
Appellant,

v. 14-2985

UNITED STATES OF AMERICA,

Appellee.

- -x

E. Joshua Rosenkranz, Orrick, Herrington & Sutcliffe LLP (Robert M. Loeb and Brian P. Goldman, Orrick, Herrington & Sutcliffe LLP, New York, NY; Guy Petrillo, Petrillo Klein & Boxer LLP, New York, NY; James M. Garland and Alexander A. Berengaut, Covington & Burling LLP, Washington, DC; Bradford L. Smith, David M. Howard, John Frank, Jonathan Palmer, and Nathaniel Jones, Microsoft Corp., Redmond, WA; *on the brief*), *for Microsoft Corporation*.

Justin Anderson, Assistant United States Attorney (Serrin Turner, Assistant United States Attorney, *on the brief*), *for* Preet Bharara, United States Attorney for the Southern District of New York, New York, NY.

Brett J. Williamson, David K. Lukmire, Nate Asher, O'Melveny & Myers LLP, New York, NY; Faiza Patel, Michael Price, Brennan Center for Justice, New York, NY; Hanni Fakhoury, Electronic Frontier Foundation, San Francisco, CA; Alex Abdo, American Civil Liberties Union Foundation, New York, NY; *for Amici Curiae* Brennan Center for Justice at NYU School of Law, American Civil Liberties Union, The Constitution Project, and Electronic Frontier Foundation, *in support of Appellant*.

Kenneth M. Dreifach, Marc J. Zwillinger, Zwillgen PLLC, New York, NY and Washington, DC, *for Amicus Curiae* Apple, Inc., *in support of Appellant*.

Andrew J. Pincus, Paul W. Hughes, Mayer Brown LLP, Washington, DC, *for Amici Curiae* BSA | The Software Alliance, Center for Democracy and Technology, Chamber of Commerce of the United States, The National Association of Manufacturers, and ACT | The App Association, *in support of Appellant*.

Steven A. Engel, Dechert LLP, New York, NY, *for Amicus Curiae* Anthony J. Colangelo, *in support of Appellant*.

Alan C. Raul, Kwaku A. Akowuah, Sidley Austin LLP, Washington, DC, *for Amici Curiae* AT&T Corp., Rackspace US, Inc., Computer & Communications Industry Association, i2 Coalition, and Application Developers Alliance, *in support of Appellant*.

Peter D. Stergios, Charles D. Ray, McCarter & English, LLP, New York, NY and Hartford, CT, *for Amicus Curiae* Ireland.

Peter Karanjia, Eric J. Feder, Davis Wright Tremaine LLP, New York, NY, *for Amici Curiae* Amazon.com, Inc., and Accenture PLC, *in support of Appellant*.

Michael Vatis, Jeffrey A. Novack, Steptoe & Johnson LLP, New York, NY; Randal S. Milch, Verizon Communications Inc., New York, NY; Kristofor T.

Henning, Hewlett-Packard Co., Wayne, PA; Amy Weaver, Daniel Reed, Salesforce.com, Inc., San Francisco, CA; Orin Snyder, Thomas G. Hungar, Alexander H. Southwell, Gibson, Dunn & Crutcher LLP, New York, NY; Mark Chandler, Cisco Systems, Inc., San Jose, CA; Aaron Johnson, eBay Inc., San Jose, CA, *for Amici Curiae* Verizon Communications, Inc., Cisco Systems, Inc., Hewlett-Packard Co., eBay Inc., Salesforce.com, Inc., and Infor, *in support of Appellant*.

Laura R. Handman, Alison Schary, Davis Wright Tremaine LLP, Washington, DC, *for Amici Curiae* Media Organizations, *in support of Appellant*.

Philip Warrick, Klarquist Sparkman, LLP, Portland, OR, *for Amici Curiae* Computer and Data Science Experts, *in support of Appellant*.

Owen C. Pell, Ian S. Forrester, Q.C., Paige C. Spencer, White & Case, New York, NY, *for Amicus Curiae* Jan Philipp Albrecht, Member of the European Parliament, *in support of Appellant*.

Owen C. Pell, Ian S. Forrester, Q.C., Paige C. Spencer, White & Case, New York, NY; Edward McGarr, Simon McGarr, Dervila McGirr, McGarr Solicitors, Dublin, Ireland, *for Amicus Curiae* Digital Rights Ireland Limited, National Council for Civil Liberties, and The Open Rights Group, *in support of Appellant*.

ORDER

Following disposition of this appeal, an active judge of the Court requested a poll on whether to rehear the case *en banc*.* A poll having been conducted and there being no majority favoring *en banc* review, rehearing *en banc* is hereby **DENIED**.

Susan L. Carney, *Circuit Judge*, concurs by opinion in the denial of rehearing *en banc*.

Dennis Jacobs, *Circuit Judge*, joined by José A. Cabranes, Reena Raggi, and Christopher F. Droney, *Circuit Judges*, dissents by opinion from the denial of rehearing *en banc*.

José A. Cabranes, *Circuit Judge*, joined by Dennis Jacobs, Reena Raggi, and Christopher F. Droney, *Circuit Judges*, dissents by opinion from the denial of rehearing *en banc*.

Reena Raggi, *Circuit Judge*, joined by Dennis Jacobs, José A. Cabranes, and Christopher F. Droney, *Circuit Judges*, dissents by opinion from the denial of rehearing *en banc*.

Christopher F. Droney, *Circuit Judge*, joined by Dennis Jacobs, José A. Cabranes, and Reena Raggi, *Circuit Judges*, dissents by opinion from the denial of rehearing *en banc*.

FOR THE COURT:
CATHERINE O'HAGAN WOLFE, CLERK

* The following active judges were recused from participating in the poll: Rosemary S. Pooler, Debra Ann Livingston, and Raymond J. Lohier, Jr.

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.

DENNIS JACOBS, *Circuit Judge*, joined by JOSÉ A. CABRANES, REENA RAGGI, and CHRISTOPHER F. DRONEY, *Circuit Judges*, dissenting from the denial of rehearing in banc:

The United States has ordered Microsoft to provide copies of certain emails pursuant to the Stored Communications Act. A magistrate judge found probable cause to believe those emails contain evidence of a crime. (The instrument functions as a subpoena though the Act calls it a warrant.) A panel of this Court directed the district court to quash the warrant as an unlawful extraterritorial application of the Act. Now, in a vote split four–four, we decline to rehear the case in banc. I respectfully dissent from the denial.

I subscribe to the dissents of Judge Cabranes, Judge Raggi, and Judge Droney, which set out in detail the doctrinal basis for the right result in this appeal. I write separately to describe an approach that is perhaps more reductionist.

I

As all seem to agree, and as the government concedes, the Act lacks extraterritorial reach. However, no extraterritorial reach is needed to require delivery in the United States of the information sought, which is easily accessible

in the United States at a computer terminal. The majority nevertheless undertakes to determine whether this case presents a forbidden extraterritorial application by first "look[ing] to the 'territorial events or relationships' that are the 'focus' of the relevant statutory provision." Majority Op., 829 F.3d at 216 (quoting *Mastafa v. Chevron Corp.*, 770 F.3d 170, 183 (2d Cir. 2014)). Oddly, the majority then holds that the relevant "territorial" "focus" is user privacy. But privacy, which is a value or a state of mind, lacks location, let alone nationality.[1] Territorially, it is nowhere. Important as privacy is, it is in any event protected by the requirement of probable cause; so a statutory focus on privacy gets us no closer to knowing whether the warrant in question is enforceable.

Extraterritoriality need not be fussed over when the information sought is already within the grasp of a domestic entity served with a warrant. The warrant in this case can reach what it seeks because the warrant was served on Microsoft, and Microsoft has access to the information sought. It need only touch some keys in Redmond, Washington. If I can access my emails from my

[1] As Judge Lynch wrote in his panel concurrence, privacy "is an abstract concept with no obvious territorial locus," and the majority's conclusion therefore "does not really help us to distinguish domestic applications of the statute from extraterritorial ones." Concurring Op., 829 F.3d at 230 n.7.

phone, then in an important sense my emails are in my pocket, notwithstanding where my provider keeps its servers.

The majority opinion relies on an implicit analogy to paper documents: "items" and "material" and "content" that are "located" and "stored" and that the government seeks to "collect" and "import." But electronic data are not stored on disks in the way that books are stored on shelves or files in cabinets. Electronic "documents" are literally intangible: when we say they are stored on a disk, we mean they are encoded on it as a pattern. At stake in this case is not whether Microsoft can be compelled to import and deliver a disk (or anything else), but whether Microsoft can be compelled to deliver information that is encoded on a disk in a server and that Microsoft can read.

The panel's approach is unmanageable, and increasingly antiquated. As explained in an article Judge Lynch cites in his concurrence (829 F.3d at 229): "[T]he very idea of online data being located in a particular physical 'place' is becoming rapidly outdated," because electronic "files [can] be fragmented and the underlying data located in many places around the world" such that the files "only exist in recognizable form when they are assembled remotely." Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. Pa. L. Rev. 373, 408

(2014). The underlying data can be fragmented or recombined, copied or transferred, for convenience or maintenance or economy – or (not incidentally) to evade the police. And all that can be done at the direction of the user or without the user's knowledge, and without a care for national boundaries, tariffs or postage. Nothing moves but information.

To enforce the warrant, there is no practical alternative to relying upon access, and no need to seek an alternative. We can conclude that warrants can reach what their recipients can deliver: if the recipient can access a thing here, then it can be delivered here; and if statutory and constitutional standards are met, it should not matter where the ones-and-zeroes are "stored."

Localizing the data in Ireland is not marginally more useful than thinking of Santa Claus as a denizen of the North Pole. Problems arise if one over-thinks the problem, reifying the notional: Where in the world is a Bitcoin? Where in my DVR are the images and voices? Where are the snows of yesteryear?

II

The majority has found no indication that Congress considered in 1986 whether a warrant issued under the Act would reach data stored on servers outside the United States; and Judge Lynch's concurrence, having recognized the

flaws in the majority opinion, calls on Congress to modernize the statute. I too would like to see Congress act, chiefly to consider certain ramifications, such as whether the United States might be vulnerable to reciprocal claims of access through local offices of American companies abroad. But we are not in a position to punt when it comes to construing a statute that either does or does not allow execution of a warrant in a case that is before us now. Holding, as the panel did, that the statute does not allow enforcement of this warrant is an interpretation of the statute, not a deferential bow to Congress. So though it would best if Congress could form a consensus on the issue, that preference is not a principle of statutory construction.

Nor can it matter how we would order legislative priorities (this would seem to be a bit down the list), or how much we would welcome bipartisan consideration of a bill that has not been enacted. Legislative proposals are myriad, and they fall as leaves. Come what may, we are left for now with the law as it is. The panel misconstrues it, and I would rehear the case in banc.

JOSÉ A. CABRANES, *Circuit Judge*, joined by DENNIS JACOBS, REENA RAGGI, and CHRISTOPHER F. DRONEY, *Circuit Judges*, dissenting from the order denying rehearing *en banc*:

An evenly-divided *en banc* court has declined to rehear a case that presents multiple questions of exceptional importance to public safety and national security.[1] I respectfully dissent.

The panel majority quashed a warrant issued under section 2703 of the Stored Communications Act ("SCA")[2] by a judicial officer of the United States upon a showing of probable cause. It erroneously concluded that the government's use of an SCA warrant to require a United States-based service "provider" (Microsoft) to disclose the contents of a customer's emails stored on servers located in Ireland was an extraterritorial application of the SCA.[3] The

---

[1] We have had occasion to observe that the decision to deny rehearing *en banc* "does not necessarily mean that a case either lacks significance or was correctly decided. Indeed, the contrary may be true. An oft-cited justification for voting *against* rehearing, perhaps counterintuitively, is that the case is '*too important* to *en banc*.'" *United States v. Taylor*, 752 F.3d 254, 256 (2d Cir. 2014) (quoting James L. Oakes, *Personal Reflections on Learned Hand and the Second Circuit*, 47 STAN. L. REV. 387, 392 (1995)) (emphasis in original). Accordingly, a reader should not give "any extra weight to a panel opinion in light of such a decision, inasmuch as the order denying rehearing may only reflect, for some judges, a general aversion to *en banc* rehearings or faith in the Supreme Court to remedy any major legal errors." *Id.* at 257.

[2] *See* 18 U.S.C. §§ 2701–12.

[3] *See* Majority Op. at 42.

panel majority ignored the fact that Microsoft lawfully had possession of the emails; that Microsoft had access to the emails in the United States; and that Microsoft's disclosure of the emails to the government would take place in the United States. In its unprecedented ruling, the panel majority has indisputably, and severely, restricted "an essential investigative tool used thousands of times a year [in] important criminal investigations around the country."[4] To top this off, the panel majority's decision does not serve any serious, legitimate, or substantial privacy interest.[5]

I.

The negative consequences of the panel majority's opinion are far reaching. It has substantially burdened the government's legitimate law enforcement efforts; created a roadmap for the facilitation of criminal activity;

[4] Petition for Rehearing and Rehearing En Banc ("En Banc Petition") 2–3. In just the second half of 2015, Google alone "received 3,716 warrants seeking data from a total of 9,412 accounts." *Id.* at 18.

[5] In his concurring opinion, Judge Lynch observes that despite Microsoft's suggestion that "this case involves a government threat to individual privacy . . . . uphold[ing] the warrant here would not undermine basic values of privacy as defined in the Fourth Amendment and in the libertarian traditions of this country." Concurring Op. at 1. As he explains, "the government complied with the most restrictive privacy-protecting requirements of the [SCA]. Those requirements are consistent with the highest levels of protection ordinarily required by the Fourth Amendment for the issuance of search warrants." *Id.* at 2.

and impeded programs to protect the national security of the United States and its allies.[6]

First, as Judge Lynch's concurring opinion explains, the panel majority's holding affords "absolute" protection from disclosure to electronic communications stored abroad, regardless of whether they are controlled by a domestic service provider and are accessible from within the United States.[7] As a result, the government can "never obtain a warrant" that would require a service provider to turn over emails stored in servers located outside the United States, regardless of how "certain [the government] may be that [emails] contain

[6] Judge Carney's opinion concurring in the order denying rehearing *en banc* does not dispute the fact that the panel majority's decision has put the safety and security of Americans at risk. Instead, in a footnote, the concurring opinion notes two sections of the SCA that it believes lessen the severity of these consequences. *Ante* at 1 n.2 (Carney, *J.*, concurring in the order denying reh'g *en banc*). The first section, 2702(b)(8), permits "[a] provider . . . [to] divulge the contents of a communication . . . to a government entity, *if the provider*, in good faith, believes that" there are exigent circumstances. *Id.* (quoting 18 U.S.C. § 2702(b)(8)) (emphasis added). The second section, 2703(e), "gives a provider immunity from civil liability for a voluntary production of content made 'in accordance with . . . [a] statutory authorization . . . .'" *Id.* at 2 n.2 (quoting 18 U.S.C. § 2703(e)). In asking us to entrust our national security to the good faith of internet service providers, I can only assume that the concurring opinion has some unstated reason for believing that Microsoft is just an atypically unpatriotic service provider and that other, more virtuous, service providers would never put their business interests ahead of public safety and national security.

[7] Concurring Op. at 4.

evidence of criminal activity, and even if that criminal activity is a terrorist plot."[8]

Second, the panel majority's opinion has created a roadmap for even an unsophisticated person to use email to facilitate criminal activity while avoiding detection by law enforcement. The Microsoft customer targeted by the government's warrant in this case indicated to Microsoft when he signed up for its service that he resided in Ireland—a representation Microsoft took at face value.[9] Because Microsoft has a policy of "stor[ing] a customer's email information . . . at datacenters located near the physical location identified by the user as its own," Microsoft automatically stored his emails on its servers in Ireland—now safely beyond the reach of an SCA warrant.[10] Based on the panel majority's holding, a criminal who resides in the United States can now check the proverbial "box" informing Microsoft that he resides in another country when signing up for service—perhaps a country without a Mutual Legal Assistance

[8] *Id.* at 4–5.

[9] Majority Op. at 8–9.

[10] *Id.*

Treaty ("MLAT") with the United States[11]—and thereby avoid having his emails disclosed to the government pursuant to an SCA warrant.

Third, the panel majority's decision has already led major service providers to reduce significantly their cooperation with law enforcement. The panel majority held that the physical location of a server containing a customer's emails determines whether an SCA warrant seeking the disclosure of those emails is an extraterritorial application of the SCA. However, electronic data storage is more complex and haphazard than the panel majority's holding assumes. Many service providers regularly "store different pieces of information for a single customer account in various datacenters at the same time, and routinely move data around based on their own internal business practices."[12] Still other providers are unable to determine "where particular data is stored or whether it is stored outside the United States."[13] Consequently, in an effort to

[11] The United States has entered into MLATs with several countries, allowing parties to the treaty to request assistance with ongoing criminal investigations, including issuance and execution of search warrants. *See id.* at 41. However, many countries do not have MLATs with the United States, *e.g.*, Indonesia and Pakistan, and law enforcement cooperation with those countries is limited. *See* Gov't Br. 48–53 (describing the inefficiencies of the MLAT process as well as its ineffectiveness in certain circumstances).

[12] En Banc Petition 18–19.

[13] *Id.*

apply the panel majority's confected holding to the technological realities of electronic data storage, major service providers are adopting restrictive disclosure policies that radically undermine the effectiveness of an SCA warrant.[14]

For example, Google will now disclose "only those portions of customer accounts stored in the United States at the moment the warrant is served."[15] Google's policy is particularly troubling because "the only [Google] employees who can access the entirety of a customer's account, including those portions momentarily stored overseas, are located in the United States."[16] As a result, law enforcement might never be able obtain data stored in Google servers abroad, even with the help of an MLAT.

Yahoo! has advised law enforcement that it "will not even preserve data located outside the United States in response to a [s]ection 2703 request."[17] This policy, as the government points out in its En Banc Petition, creates "a risk that

---

[14] *See Id.* 17–19; *see also* Orin Kerr, *The Surprising Implications of the Microsoft/Ireland Warrant Case*, WASH. POST: THE VOLOKH CONSPIRACY (Nov. 29, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/11/29/the-surprising-implications-of-the-microsoftireland-warrant-case.

[15] En Banc Petition 19.

[16] *Id.*

[17] *Id.*

data will be moved or deleted before the United States can seek assistance from a foreign jurisdiction, much less actually serve a warrant and secure the data."[18]

II.

The baleful consequences of the panel's decision are compelled neither by the text of the statute nor by our precedent. The panel majority arrived at its damaging holding because it adopted a flawed reading of the SCA.

The second step of the two-step framework for analyzing extraterritoriality issues set forth in *Morrison v. National Australia Bank Ltd.*, 561 U.S. 247 (2010), and *RJR Nabisco, Inc. v. European Community*, 136 S. Ct. 2090 (2016), was the determinative issue in this case.[19] At step two, a court must "determine whether

---

[18] *Id.*

[19] The first step of the extraterritorial analysis is "to determine whether the relevant statutory provision contemplates extraterritorial application." Majority Op. at 22 (citing *Morrison*, 561 U.S. at 262–65). Because the government conceded at oral argument that the SCA lacks extraterritorial application, *id.*, there is no need to pursue the point. To the extent the panel majority did so in a lengthy discussion of the SCA's use of the word "warrant" in section 2703, *see id.* at 25–31, which then informs its step-two "focus" analysis, it is appropriate to note concern with the reasoning.

The panel majority conflates SCA disclosure warrants with traditional search warrants. While the latter authorize government action as to *places*, the former authorize government action on *persons*. The fact that warrants generally do not authorize government searches of places outside the United States—a limitation grounded in respect for sovereignty, not privacy, *see, e.g.*, *The Apollon*, 22 U.S. (9 Wheat.) 362, 371 (1824) (Story, J.); Restatement (Third) of Foreign Relations Law § 432(2); *see also In re Terrorist Bombings of U.S. Embassies in E. Africa*, 552 F.3d 157, 167–72 (2d Cir. 2008)—does not support a conclusion that warrants are impermissibly applied extraterritorially

the case involves a domestic application of the statute," which "we do . . . by looking to the statute's 'focus'" and by identifying where "the conduct relevant to the statute's focus occurred."[20] Here, the panel majority explained that the "focus" of the SCA is user privacy,[21] and in a single sentence, identified the location of the conduct relevant to that focus: "[I]t is our view 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

---

when they compel persons within the United States to disclose property lawfully in their possession anywhere in the world. *Cf. Linde v. Arab Bank, PLC*, 706 F.3d 92, 109 (2d Cir. 2013) (Carney, *J.*) (observing that the Supreme Court has held that "the operation of foreign law 'do[es] not deprive an American court of the power to order a party subject to its jurisdiction to produce evidence even though the act of production may violate that [law]." (quoting *Societe Nationale Industrielle Aerospatiale v. U.S. Dist. Court*, 482 U.S. 522, 544 n. 29 (1987)). In that sense, a disclosure warrant is more akin to a subpoena, *see, e.g.*, *Marc Rich & Co. A.G. v. United States*, 707 F.2d 663, 668–70 (2d Cir. 1983) (holding that persons in the United States can be required to retrieve subpoenaed material from abroad), *but* with the important added protection of a probable cause showing to a neutral magistrate. Thus, the panel majority is simply wrong in concluding that "a warrant protects *privacy* in a distinctly territorial way." Majority Op. at 26 (emphasis added). Warrants protect privacy through the Fourth Amendment requirement that they issue only upon probable cause. *See* Concurring Op. at 1–3.

By failing to distinguish between search warrants as to places and disclosure warrants directed to persons, and between sovereignty and privacy, the panel majority construes "warrant" as used in the SCA to yield the perverse result of affording greater privacy protection to foreign nationals and Americans who say they reside abroad than to resident United States citizens with respect to electronic communications in the lawful possession of a United States service provider.

[20] *RJR Nabisco*, 136 S. Ct. at 2101.

[21] *See* Majority Op. at 32–39.

agent of the government."[22] Because the emails at issue were stored on a server in Ireland, the panel majority concluded that the warrant seeking the disclosure of those emails was an extraterritorial application of the SCA.[23] Not so.

Even if the "focus" of the SCA is user privacy, a plain reading of the statute makes clear that the conduct relevant to the SCA's "focus," and which the SCA seeks to regulate, is a provider's *disclosure* or *non-disclosure* of emails to third parties, not a provider's *access* to a customer's data. Here, Microsoft's disclosure

---

[22] *Id.* at 39. Judge Carney's opinion concurring in the order denying rehearing *en banc* reiterates the panel majority's conclusion—that, "the locus of the SCA's privacy protections [is] at the place of data storage"—but again provides little or no explanation for how or why the statutory language permits such a reading. *Ante* at 4 (Carney, *J.*, concurring in the order denying reh'g *en banc*). It offers only the sphinx-like explanation that "§ 2701, by proscribing unauthorized access to storage facilities, not only limits disclosure but also 'shelters the communications' integrity.'" *Id.* at 5 (quoting Majority Op. at 35). Conversely, and as the concurring opinion itself notes, those of us dissenting from the denial of *en banc* review "offer[ ] a detailed recitation of the available statutory support for [the] conclusion" that the conduct relevant to the SCA's focus occurs at the place of disclosure. *Id.* at 6.

[23] Judge Carney's *en banc* concurrence asserts that the panel majority's "reading of the SCA did no more than adhere to the dictates of *Morrison* in construing the SCA." *Ante* at 3 (Carney, *J.*, concurring in the order denying reh'g *en banc*). I disagree. Instead of locating support for its legal conclusion in the text or structure of the SCA, the concurring opinion, like the panel majority's opinion, fixates on its unsubstantiated belief that the warrant at issue here raises "concerns of sovereignty and international comity." *Id.* at 4. They both then conclude, based primarily on that misconception, that the warrant at issue must be an extraterritorial application of the SCA. *Morrison*, however, does not permit a court to conclude that a particular application of a statute is extraterritorial simply because it believes that the application threatens international comity. Rather, step two of the *Morrison* framework directs courts to examine the statutory language. *See Morrison*, 561 U.S. at 266–67.

of emails to the government would take place at its headquarters in the United States. Therefore, had the panel majority correctly identified the conduct relevant to the SCA's "privacy focus," it would have concluded that the warrant at issue was a domestic application of the SCA.[24]

A brief examination of the text and structure of the SCA leads inexorably to the conclusion that the conduct relevant to the SCA's "privacy focus" is its regulation of *disclosures* by providers to third-parties. As the panel majority

---

[24] According to the *en banc* concurrence, the panel majority considered and rejected my suggested holding partly because that holding "ignores situations in which the effects outside the United States are less readily dismissed." *Ante* at 8 (Carney, *J.*, concurring in the order denying reh'g *en banc*). As far as I understand it, the concurring opinion asserts the belief that the facts of this case are too sympathetic to my interpretation of the law and that only under alternative, entirely fictional, circumstances would the true menace of my position be revealed. It then devises a hypothetical warrant that purports to show how my suggested holding permits the authorization of warrants with too limited a nexus to the United States: an SCA warrant requiring a "United States . . . branch office of an Irish service provider" to disclose electronic information stored in Ireland but accessible in the United States that belonged to an account "opened and established in Ireland by an Irish citizen," the disclosure of which would breach Irish law. *Id*.

This hypothetical is too clever by half. In attempting to construct the most shocking warrant conceivable, the concurring opinion omits two critical facts, both of which are required under my understanding of the law. First, a judicial officer of the United States would have to issue the warrant upon a finding of probable cause to believe that the information being sought was related to criminal activity occurring within the United States. Second, the provider would have to disclose the targeted information to the government inside the United States. Thus, if all of the conditions necessary for a valid SCA warrant are satisfied, there is no basis for concluding that even Judge Carney's imagined warrant, not to mention the warrant at issue, is an extraterritorial application of the SCA.

observes, "the first three sections of the SCA contain its major provisions."[25] The first of those sections, section 2701, addresses "[u]nlawful access to stored communications."[26] Section 2701 is the *only* major provision of the SCA to specifically limit *access* to customer communications. Although the panel majority fails to explain adequately why the "invasion of the customer's privacy takes place . . . where the customer's protected content is *accessed*,"[27] section 2701 is the only plausible textual basis for the panel majority's bizarre holding.

However, while section 2701 prohibits "[u]nlawful access" (most obviously hacking), it recognizes that providers have standing authority to *access* a customer's electronic communications.[28] In fact, section 2701(c) expressly exempts from its restrictions on *access* "conduct authorized . . . by the person or entity providing a wire or electronic communications service," *i.e.*, the provider.[29] It is unreasonable, therefore, for the panel majority to conclude that a provider's

[25] *Id.* at 35; *see* 18 U.S.C. §§ 2701–03

[26] 18 U.S.C. § 2701.

[27] Majority Op. at 39 (emphasis added).

[28] 18 U.S.C. § 2701

[29] *Id.* § 2701(c)(1) (emphasis added).

lawful access to a customer's emails is the conduct relevant to the SCA's "privacy focus."[30]

On the other hand, section 2702 expressly prohibits, with some exceptions, a provider from "*disclos[ing]*" a customer's communications.[31] For example, section 2702(a) sets forth three "[p]rohibitions" that must be followed by servicer providers like Microsoft.[32] Each prohibition states that the provider "shall not knowingly *divulge*" certain information, such as the contents of a communication, unless an exception in subsection (b) or (c) applies.[33] In turn, section 2703 specifically empowers the government to "require the *disclosure* by a provider . . . of the contents of a[n] . . . electronic communication . . . pursuant to a warrant."[34]

Considering sections 2701, 2702, and 2703 together, it is clear that the SCA protects user privacy by prohibiting unlawful access of customer communications (such as hacking), and by regulating a provider's *disclosure* of

---

[30] The panel majority characterizes a service provider that "access[es]" a user's email pursuant to an SCA warrant as "an agent of the government." Majority Op. at 29, 39. But, the legal authorities cited by the panel for the proposition that a private party who assists the government in conducting a search and seizure "becomes an agent of the government," *id.* at 29, do not involve circumstances, such as those here, where the private party already had possession of the relevant property.

[31] *Id.* §§ 2702–03 (emphasis added).

[32] *See id.* § 2702(a)(1)–(3).

[33] *Id.* (emphasis added).

[34] *Id.* § 2703(a) (emphasis added).

customer communications to third parties. Inasmuch as section 2701's limitations on *access* specifically do not apply to providers, it is only when a provider *divulges* the content of a user's communication to a third party that the provider puts a user's privacy at risk. It is not a mere coincidence that the SCA recognizes a provider's standing authority to *access* a user's communications and, at the same time, prohibits a provider from *disclosing* those communications to third-parties except as authorized by sections 2702 and 2703. Accordingly, the panel majority's focus on *access* (instead of on *disclosure)* is entirely misplaced.[35]

Put another way, Microsoft did not need a warrant to take possession of the emails stored in Ireland. Nor did it need a warrant to move the emails from Ireland to the United States. It already had possession of, and lawful *access* to, the targeted emails from its office in Redmond, Washington. Only Microsoft's

[35] Neither the panel majority's opinion nor the *en banc* concurrence explains why "privacy" is better served by looking to a provider's *access* rather than its *disclosure*. They just assume the point. *See ante* at 13 (Carney, *J.*, concurring in the order denying reh'g *en banc*) ("The better approach . . . is one that looks to the step taken before disclosure—access—in determining privacy's territorial locus."); Majority Op. at 39. Both the panel majority's opinion and the *en banc* concurrence also fail to explain why the physical location of the datacenter is the legal point of *access*, rather than the location from where the service provider electronically gains *access* to the targeted data, which, in this case, is the United States. Evidently, it is so (again) because the panel majority and the concurrence say it is so. *See ante* at 4 (Carney, *J.*, concurring in the order denying reh'g *en banc*) ("[T]he locus of the SCA's privacy protections [is] at the place of data storage."); Majority Op. at 39. Naked assertions, however, do not the law make.

disclosure of the emails to the government would have been unlawful under the SCA absent a warrant.[36]

***

In sum, the government obtained a warrant based on a showing of probable cause before a judicial officer of the United States. That warrant required Microsoft's office in Redmond, Washington, to disclose certain emails that happened to be electronically stored in its servers abroad, but to which Microsoft had immediate access in the United States. Because the location of a provider's *disclosure* determines whether the SCA is applied domestically or extraterritorially, the enforcement of the warrant here involved a domestic application of the SCA. The panel should have affirmed the District Court's denial of Microsoft's motion to quash.

For the foregoing reasons, I dissent from the order denying rehearing *en banc*. I trust that the panel's misreading of this important statute can be rectified

[36] To the extent the panel majority concludes that the SCA does not apply extraterritorially to compel a provider's disclosures pursuant to section 2703, its place-of-access reasoning raises concerns about the extraterritorial reach of protections from unlawful access and disclosures afforded by sections 2701 and 2702. Such a concern might be avoided if the statute is construed to reach, at least, the conduct of persons within the jurisdiction of the United States. This further concern only reinforces the need for *en banc* review.

as soon as possible by a higher judicial authority or by the Congress of the United States.[37]

[37] Ultimately, Judge Carney's concurring opinion suggests that rehearing *en banc* is unnecessary because the panel majority's holding was compelled by an anachronistic statute and an inflexible framework for analyzing questions of extraterritoriality. *Ante* at 13–14 (Carney, *J.*, concurring in the order denying reh'g *en banc*). It also notes that some Members of Congress have introduced a bill purporting to resolve all of our concerns with the statute. *Id.* at 2 n.3. I submit that rehearing *en banc* is necessary precisely because the panel majority misread the SCA and misapplied the extraterritoriality framework set forth in *Morrison*. Where a decision of our court has unnecessarily created serious, on-going problems for those charged with enforcing the law and ensuring our national security, and where a legislative remedy is entirely speculative, we should not shirk our duty to interpret an extant statute in accordance with its terms.