855 F.3d 53
United States Court of Appeals,
Second Circuit.

In the MATTER OF a WARRANT TO SEARCH A CERTAIN E-MAIL ACCOUNT CONTROLLED AND MAINTAINED BY MICROSOFT CORPORATION
Microsoft Corporation, Appellant,
v.
United States of America, Appellee.

14-2985
|
January 24, 2017

Attorneys and Law Firms

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.

***54** 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.

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.

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.

***55** 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 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, 130 S.Ct. 2869, 177 L.Ed.2d 535 (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 the extraterritoriality analysis set forth as a canon of construction in *Morrison* and recently developed further in *RJR Nabisco, Inc. v. European Community*, —— U.S. ——, 136 S.Ct. 2090, 195 L.Ed.2d 476 (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 ***56** 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 systemaffords.

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]

***57** 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 of disclosure, on U.S. soil.[6] Thus, so long as (1) the warrant ***58** 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 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 "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, 130 S.Ct. 2869 (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, 111 S.Ct. 1227, 113 L.Ed.2d 274 (1991) (observing ***59** that presumption against extraterritoriality "serves to protect against unintended clashes between our laws and those of other nations").

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 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 62 (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 ***60** *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 ***61** 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 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 ***62** 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 ***63** 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 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; 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 ***64** emails stored in servers located outside the United States, regardless of how "certain [the government] may be that [emails] contain 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 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 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 ***65** 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 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, 130 S.Ct. 2869, 177 L.Ed.2d 535 (2010), and *RJR Nabisco, Inc. v. European Community*, —— U.S. ——, 136 S.Ct. 2090, 195 L.Ed.2d 476 (2016), was the determinative issue in this case.[19] At step two, a court ***66** must "determine whether 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 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 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]

***67** 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 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 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] ***68** ... 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 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 *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 as soon as possible by a higher judicial authority or by the Congress of the United States.[37]

***69** Reena Raggi, Circuit Judge, joined by Dennis Jacobs, José A. Cabranes, and Christopher F. Droney, Circuit Judges, dissenting from the order denying rehearing en banc:

In this case, a panel of the court quashes a compelled-disclosure warrant issued under the Stored Communications Act ("SCA") by a neutral magistrate and supported by probable cause to think that the information demanded is evidence of a crime. *See* 18 U.S.C. § 2703(a). The ground for decision is the presumption against extraterritoriality, *see Morrison v. Nat'l Australia Bank Ltd.*, 561 U.S. 247, 255, 130 S.Ct. 2869, 177 L.Ed.2d 535 (2010), which the panel construes to allow United States corporation Microsoft to refuse to disclose subscriber communications in its possession and responsive to the warrant because Microsoft, for its own business reasons and unbeknownst to its subscriber, has chosen to store the communications in Ireland. The panel does not simply set a *higher* bar for the government to secure such electronic communications. Rather, it erects an "*absolute*" bar so that "the government can never obtain a warrant that would require Microsoft," or any other U.S.-based service provider, to turn over electronic communications stored abroad, "however certain it may be that they contain evidence of criminal activity, and even if that criminal activity is a terrorist plot." *Microsoft Corp. v. United States* ("*Microsoft*"), 829 F.3d 197, 224 (2d Cir. 2016) (Lynch, J., concurring in the judgment) (emphasis in original).[1] This ruling merits *en banc* review. To the extent an equally divided court today denies such review, I respectfully dissent.

1. Matter of Exceptional Importance

The panel's ruling, the reasoning informing it, and its disturbing consequences raise questions "of exceptional importance to public safety and national security." Cabranes, J., Op. Dissenting from Denial of Reh'g En Banc ("Cabranes, J., Op."), *ante* at 62. The panel nevertheless urges us to forego *en banc* review because the SCA is outdated and overdue for congressional revision. *See Microsoft*, 829 F.3d at 201; Carney, J., Op. Concurring in Denial of Reh'g En Banc ("Carney, J., Op."), *ante* at 55 & n.3. I am not persuaded.

This is not a case where some legal principle (*e.g.*, standing, mootness) allowed the panel to avoid applying the SCA, ***70** thereby affording Congress time to enact new legislation. This is a case where the panel reached the merits and construed the SCA to foreclose altogether § 2703(a) warrants requiring United States service providers to disclose electronic communications stored overseas. This construction now controls the SCA's application in this circuit. In its Petition for Rehearing, the government details the immediate and serious adverse consequences of such a ruling. *See* Gov't Pet. for Reh'g at 18–19; *see also* Cabranes, J., Op., *ante* at 63–65. These consequences cannot be attributed to deficiencies in the SCA. Rather, they derive from the panel's conclusion—mistaken in my view—that the SCA is impermissibly being applied extraterritorially when a § 2703(a) warrant requires a United States service provider to disclose electronic communications that it has elected to store abroad. It is simply unprecedented to conclude that the presumption against extraterritoriality bars United States courts with personal jurisdiction over a United States person from ordering that person to produce property in his possession (wherever located) when the government has made a probable cause showing that the property is evidence of a crime. This alone warrants *en banc* review.

2. The Panel's Discussion of "Warrant"

Several aspects of the panel's extraterritoriality analysis require particular review. The first is the panel's lengthy discussion of why Congress's "use of the term of art 'warrant' " in the SCA manifests an intent for the statute to operate only domestically. *Microsoft*, 829 F.3d at 212. At the outset, I note that there was no need for the panel to locate *domestic* intent in the SCA; it is presumed in the absence of a showing of express *extraterritorial* intent, which the government concedes is absent here. *See Morrison v. Nat'l Australia Bank Ltd.*, 561 U.S. at 255, 130 S.Ct. 2869. The panel majority's "warrant"

discussion, however, is not simply unnecessary. It is also flawed in ways that lay an unsound foundation for the panel's ensuing identification of statutory "focus."

Notably, the panel majority concludes that Congress's use of the term "warrant" in § 2703 signals its intent to invoke all of the "traditional, domestic connotations" that pertain to traditional search warrants. *Microsoft*, 829 F.3d at 213. But, as Judge Lynch observes, a § 2703(a) warrant is not a traditional warrant. *Id.* at 226 (Lynch, J., concurring in the judgment). It does not authorize federal agents to *search* any premises or to *seize* any person or materials. Rather, it authorizes a federal agent to require a service provider to disclose materials in its possession. The difference is significant to identifying where a warrant is being executed. Because a search warrant is executed with respect to a *place*—the place to be searched—the presumption against extraterritoriality expects that place to be within United States territory. By contrast, because a § 2703(a) warrant is executed with respect to a *person*—the person ordered to divulge materials in his possession—the presumption against extraterritoriality expects that person to be within United States territory and subject to the court's jurisdiction. If the person is so present, execution of the warrant as to him is a domestic application of United States law without regard to from where the person must retrieve the materials ordered disclosed. Indeed, if that were not so, subpoenas requiring persons in this country to produce materials that they must retrieve from abroad could not be enforced, a position contrary to well established law. *See, e.g.*, *Marc Rich & Co., A.G. v. United States*, 707 F.2d 663, 668–70 (2d Cir. 1983); *United States v. Bank of Nova Scotia (In re Grand Jury Proceedings)*, 740 F.2d 817, 826–29 (11th Cir. 1984).

***71** Thus, I respectfully submit that the panel majority's extraterritoriality analysis starts with the mistaken equation of § 2703(a) warrants with traditional search warrants. This, in turn, leads to the mistaken conclusion that "a warrant protects privacy in a distinctly territorial way." *Microsoft*, 829 F.3d at 212.

As to the latter point, the reason United States search warrants do not apply extraterritorially has to do with *sovereignty*, not *privacy*. Since before the republic, the law of nations has recognized that one sovereign cannot unilaterally enforce its criminal laws within the territory of another.[2] But a defendant's expectations of privacy do not preclude evidence so obtained from being used in a United States prosecution. *See In re Terrorist Bombings of U.S. Embassies in E. Africa*, 552 F.3d 157, 176–77 (2d Cir. 2008). Thus, it is respect for sovereign independence that has prompted us to observe that "search warrants intended to have extraterritorial effect ... would have dubious legal significance, if any, in a foreign nation." *Id.* at 171. But this observation, quoted by the panel majority, does not support its ensuing conclusion that, "[a]ccordingly, a warrant protects *privacy* in a distinctly territorial way." *Microsoft*, 829 F.3d at 212 (emphasis added).

As Judge Lynch explains, how warrants protect *privacy* is through the Fourth Amendment requirement that they issue only "upon probable cause." U.S. Const. amend. IV; *see Microsoft*, 829 F.3d at 223 (Lynch, J., concurring in the judgment). Indeed, to the extent the SCA's legislative history shows Congress's intent to extend privacy protections, specifically, protections "analogous to those provided by the Fourth Amendment," to certain electronic communications, *Microsoft*, 829 F.3d at 206 (quoting Gov't Br. at 29), one might better understand Congress to have used the term "warrant" in § 2703(a) to ensure that certain disclosures would be compelled only upon a showing of probable cause. Thus, when a § 2703(a) warrant supported by probable cause is executed on a person within the jurisdiction of the United States, the SCA is being applied domestically without regard to the location of the materials that the person must divulge.

As Judge Cabranes observes, by failing to recognize these distinctions (a) between search warrants directed to particular locations and § 2703(a) warrants directed to particular persons, and (b) between the values of sovereignty and privacy, the panel majority construes "warrant" as used in § 2703 to yield a perverse result: affording *greater* privacy protection to foreign citizens and Americans who claim to reside abroad than to resident U.S. citizens. *See* Cabranes, J., Op., *ante* at 65 n.19. This troubling result and the reasons leading to it warrant *en banc* review.

3. The Focus of the Statute

Where, as here, the government does not argue that Congress intended for ***72** § 2703(a) to apply extraterritorially, the determinative question asks whether the domestic contacts associated with that statutory provision are sufficient to avoid triggering the presumption against extraterritoriality. To answer that

question, a court looks to "the territorial events or relationships" that are the "focus" of the relevant statutory provision. *Mastafa v. Chevron Corp.*, 770 F.3d 170, 184 (2d Cir. 2014) (alterations omitted); *Morrison v. Nat'l Australia Bank Ltd.*, 561 U.S. at 266–68, 130 S.Ct. 2869. The panel majority identifies "privacy" as the focus of § 2703(a)'s warrant requirement. *Microsoft*, 829 F.3d at 217. It then reasons that because the § 2703(a) warrant here sought disclosure of the electronic communications of a Microsoft customer, and because Microsoft stored those communications in Dublin, "[t]he content to be *seized* is stored in Dublin." *Id.* at 220 (emphasis added). This in turn leads it to conclude 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 agent of the government*." *Id.* (emphasis added). Accordingly, it concludes that the § 2703(a) warrant is being executed in Ireland in violation of the presumption against extraterritoriality.

This reasoning raises several concerns.

First, I cannot agree that a person who is compelled by a § 2703(a) warrant to disclose to the government materials already in that person's possession is "seiz[ing]" anything as an agent of the government. *See id.* The cases cited by the panel majority identify such agency where property is *not* already in an actor's possession. In such circumstances, but for authorizing law or warrant, the actor could not lawfully take possession of—*i.e.*, seize—third-party materials. That is not the case here. Microsoft did not need any warrant from the United States to take possession of the subscriber communications it had stored in Ireland. Nor did it need such a warrant to transfer those communications from Ireland to the United States. Indeed, it did not need the approval of Irish authorities or even of its subscriber to take such action. Thus, it is simply wrong to characterize Microsoft's actions in retrieving customer electronic data in Ireland as "Microsoft's *execution* of the warrant," much less as a *seizure* by Microsoft. Carney, J., Op., *ante* at 56 (emphasis added); *see Microsoft*, 829 F.3d at 220. The § 2703(a) warrant here at issue was executed by *federal authorities*, who were thereby authorized to compel Microsoft to *disclose* communications already lawfully in its possession. Such disclosure by Microsoft would otherwise have been prohibited by 18 U.S.C. § 2702(a). But the only territorial event that needs to be warranted under the SCA is disclosure. No warrant was needed for Microsoft lawfully to access material on its Dublin servers from the United States. Nor is a different conclusion supported by the panel majority's observation that our court "has never upheld the use of a subpoena to compel a recipient to produce an item under its control and located overseas when the recipient is merely a caretaker for another individual or entity and that individual, not the subpoena recipient, has a protectable privacy interest in the item." *Microsoft*, 829 F.3d at 215. The question whether the caretaker's actions respecting materials in his possession constitute a "search" or "seizure" undertaken as an agent of the government does not turn on whether the item is located here or overseas. Indeed, as Judge Lynch states, we have upheld the use of a subpoena to compel a caretaker to produce client materials in its domestic possession. *See id.* at 228 n.5 (Lynch, J., concurring in the judgment) (citing *In re Horowitz*, 482 F.2d 72 (2d Cir. 1973)). Such ***73** a conclusion would not have been possible if the caretaker's actions respecting materials in his possession equated to a "search" or "seizure" undertaken as an agent of the government.

Thus, we need to convene *en banc* to clarify that a service provider who complies with a § 2703(a) warrant compelling disclosure of communications in his lawful possession does not thereby conduct a search or seizure as the agent of the government.

Second, I also cannot agree with the panel that *privacy* is the focus of § 2703 and that subscriber privacy would be invaded *in Ireland* were Microsoft to access its subscriber files there. To the extent § 2702(a) generally prohibits a service provider from knowingly disclosing subscribers' electronic communications to third parties, that provision might be understood to focus on enhancing subscriber privacy. But § 2703 identifies circumstances when the government nevertheless "may require" service providers to disclose their subscribers' communications. This gives some force to the government's argument that the focus of § 2703 is compelled *disclosure*, not enhanced *privacy*. *See* Gov't Pet. for Reh'g at 11–12 (noting that focus inquiry is "provision-specific" and citing *RJR Nabisco, Inc. v. European Cmty.*, ––– U.S. ––––, 136 S.Ct. 2090, 2101–11, 195 L.Ed.2d 476 (2016)). *But see Microsoft*, 829 F.3d at 218–19 (rejecting disclosure focus argument).

Even assuming that the enhanced privacy and compelled disclosure provisions of the SCA are two sides of the same coin, I think the panel errs in concluding that the privacy afforded by the SCA would be invaded by Microsoft's access of its own files in Dublin rather than

by its subsequent disclosure of subscriber communications in the United States.

As already stated, Microsoft is entitled to access and to move subscriber communications at will, even without consulting its subscriber. Such actions by Microsoft disclose nothing to the government about the existence or content of such communications. The only privacy interest afforded by § 2702(a), however, is against such disclosure. The statute provides no privacy right against Microsoft's own handling of communications short of such disclosure. Thus, contrary to the panel, I think that, even if privacy is the focus of §§ 2702 and 2703, the territorial event that is the focus of that privacy interest is the service provider's disclosure of the subscriber communications to a third party—whether in violation of § 2702(a) or as authorized by warrant under § 2703(a). It is where that disclosure occurs that determines whether these statutory provisions are being applied domestically or extraterritorially.

Here, there is no question that the challenged § 2703(a) warrant issued, was served on Microsoft in, and required disclosure in the United States. Thus, even if "privacy" is the statute's "focus," the challenged warrant here applies the statute domestically, not extraterritorially. We should say so *en banc*.

4. Concluding Observations

Two final points. As Judge Cabranes observes, and Judge Carney seems to agree, the same reasoning that leads the panel to conclude that § 2703(a) warrants cannot reach communications that Microsoft has stored in Ireland might also preclude affording § 2702(a) privacy protections to such materials. *See* Cabranes, J., Op., *ante* at 68 n.36; Carney, J., Op., *ante* at 57 n.6. But if § 2702(a) protections do not apply here, does the government even need a § 2703(a) warrant? Could it simply proceed by subpoena? *See* ***74** *Marc Rich & Co., A.G. v. United States*, 707 F.2d at 668–70; *United States v. Bank of Nova Scotia (In re Grand Jury Proceedings)*, 740 F.2d at 826–29. I think the government does need a § 2703(a) warrant because I understand both § 2702(a) protections and § 2703(a) warrants to exercise government authority domestically on persons subject to United States jurisdiction. To the extent, however, that the panel's extraterritoriality reasoning might allow a United States service provider such as Microsoft to flout not only § 2703(a) warrants but also § 2702(a) protections simply by moving materials abroad, the need for *en banc* review is only heightened.

My second point is not unrelated. The panel concludes that, because the Congress that enacted the SCA could not have foreseen the technological context in which this case arises, the focus of the statute cannot be domestic disclosure of data that a service provider in the United States accesses from abroad. Therefore, the warrant should be quashed. It seems to me this allows the first prong of analysis—did Congress intend extraterritoriality?—to be determinative of the second—is the statute being applied extraterritorially in the case at hand? In fact, the two steps of analysis are distinct. *See Morrison v. Nat'l Australia Bank Ltd.*, 561 U.S. at 266, 130 S.Ct. 2869. Whatever Congress may have foreseen about advances in electronic communications, I think, for the reasons already stated, that the SCA is being applied domestically here. The privacy protection afforded by § 2702(a) is against unauthorized *disclosure* to third parties. But a § 2703(a) warrant here specifically authorizes federal agents to compel disclosure in the United States. Further, the party from whom such disclosure is being compelled is a United States service provider subject to the personal jurisdiction of United States courts. In short, this is not the case hypothesized by the panel where the government might use a § 2703(a) warrant to demand communications *stored abroad* from a *foreign service provider* relating to a *foreign subscriber*. *See, e.g.*, *Microsoft*, 829 F.3d at 231–32 (Lynch, J., concurring in the judgment); Carney, J., Op., *ante* at 59. When such a case comes before us, we can certainly consider whether a court with personal jurisdiction over the foreign service provider can issue a § 2703(a) warrant compelling it to disclose in the United States communications stored abroad. But, in this case, where the warrant is directed to a United States provider over whom there is personal jurisdiction for production in the United States of specified communications on a federal magistrate's identification of probable cause, I simply do not think we have an extraterritorial application of U.S. law.

For the foregoing reasons, this court *en banc* should enforce, not quash, the challenged § 2703(a) warrant.

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

The majority opinion undertook the daunting task of attempting to apply a statute enacted decades ago to present technology. For example, who knew in 1986 that electronic mail—"email"—would become such a primary means of communication that its commercial providers would have millions of servers across the world to store and manage those communications? Or that the recipient of the warrant here—Microsoft—would itself manage over one million server computers, located in over forty countries, used by over one billion customers? Such developments in electronic communications could not have been anticipated at the time of the statute's adoption. Indeed, the task of applying statutes and rules from many years ago to ***75** unanticipated advances in technology has been undertaken in other contexts with much difficulty. *See, e.g.*, *United States v. Ganias*, 824 F.3d 199, 219–21 (2d Cir. 2016) (*en banc*). Thus, although I agree that reconsideration *en banc* should have occurred, I do so while recognizing the majority's efforts to solve the vexing issues presented here.

I dissent, though, from the denial of *en banc* in this case for three reasons. First, the privacy interests that are the focus of many aspects of the Stored Communications Act ("SCA") are protected in this context by its warrant requirement. Second, the activity that is the focus of the disclosure aspects of the SCA would necessarily occur in the United States where Microsoft is headquartered and where it would comply with the § 2703 warrant, not in the foreign country where it has chosen to store the electronic communications of its customers; also, the provisions of the statute concerning the mechanics of disclosure of these communications are unrelated to its privacy provisions. Third, the prudent course of action is to allow the warrants to proceed, and if Congress wishes to change the statute, it may do so while important criminal investigations continue.

When determining whether a statute applies extraterritorially, a court must read the statute provision by provision, not as a whole. *RJR Nabisco, Inc. v. European Community*, —— U.S. ——, 136 S.Ct. 2090, 2103, 195 L.Ed.2d 476 (2016) (analyzing provisions individually to determine the focus of each). The court is then tasked with "determin[ing] whether the case involves a domestic application of the statute, and [does] this by looking to the statute's 'focus.' " *Id.* at 2101.

As the majority opinion notes, the SCA was broadly focused on the privacy concerns of electronic communications and the parties to those communications. *See* Maj. Op. at 216–220. But Congress addressed those concerns through the warrant requirement in the SCA. *See* 18 U.S.C. § 2703. That requirement provides protection for individual privacy interests by requiring the Government to make an adequate showing of probable cause of evidence of a crime or property used to commit a crime to a judge—a well-established standard of Fourth Amendment protection. *See id.*; Fed. R. Crim. P. 41(c); U.S. Const. amend. IV ("[N]o warrants shall issue, but upon probable cause."); *Camara v. Mun. Court of City & Cnty. of S.F.*, 387 U.S. 523, 528, 87 S.Ct. 1727, 18 L.Ed.2d 930 (1967) (explaining that purpose of Fourth Amendment's probable cause requirement "is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials").

Furthermore, the provisions of the SCA concerning the means of disclosure following obtaining the warrant are quite separate from the privacy components of the SCA. Section 2703 includes a number of specific disclosure provisions, which state it is the *provider* of the electronic communication service that is the source of the records sought by the Government either pursuant to the warrant or the other means provided by that section to properly obtain the electronic communications. *See id.* § 2703 (a) ("A governmental entity may require the disclosure *by a provider* of electronic communication service of the contents of a wire or electronic communication...") (emphasis added); § 2703 (b)(1) ("A governmental entity may require *a provider* of remote computing service to disclose the contents of any wire or electronic communication ...") (emphasis added); § 2703 (c)(1) & (2) (both describing disclosure by providers); § 2703 (g) (same).

***76** Thus, the only permissible reading of § 2703 is that it is the location of the provider of the electronic communication service that is relevant to determining whether the SCA is being applied extraterritorially under *RJR Nabisco*. Microsoft is headquartered in the United States, and there is no question that it would make the disclosure mandated by the § 2703 warrant in this country.

It makes no difference that Microsoft has chosen to store some electronic communications in other countries. That decision is based on its own business considerations, not privacy concerns for its customers. Microsoft has possession and immediate access to those emails regardless of where it chose to store them. Thus, the second prong of the *RJR Nabisco* test is satisfied here: the

disclosure of the electronic communications occurs in the United States, when Microsoft honors the warrant by disclosing those communications.

It is also important to note that the interests of foreign internet electronic communication service providers, whose headquarters are abroad and whose customers choose to subscribe to those services with the knowledge that the provider is located outside the United States, are not at stake here. If the emails sought by the Government in this case were maintained by a foreign-based internet service provider, the situation would be quite different. Here, however, the majority's concerns regarding "the interests of comity that ... ordinarily govern the conduct of cross-boundary criminal investigations," Maj. Op. at 221, are overstated when the warrant is served on a U.S.-based electronic communication service provider for stored emails of a customer who *chose* to have a U.S.-based electronic communication service provider furnish his email service.

There is a real and practical component to the denial of *en banc* review of this case. This is a case that turns on statutory interpretation under *RJR Nabisco* rather than responding to a direct challenge to the constitutionality of the SCA or its disclosure provisions. The denial of *en banc* review hobbles both this specific Government investigation as well as many others, important not only to the United States but also foreign nations. The Government's interest in continuing critical investigations into criminal activity is manifest. If Congress wishes to revisit the privacy and disclosure aspects of § 2703, it is free to do so when it chooses to do so. Until that time, this Court should allow the warrants to compel disclosure pursuant to § 2703 as it exists, and allow the Government to do its job in investigating serious criminal activity.

For these reasons, I respectfully dissent from the denial of *en banc* review.

All Citations

855 F.3d 53 (Mem)

Footnotes

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

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 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).

4 This approach, in which we considered several numbered sections of the SCA, is not 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 61 (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 65 n.19 (Cabranes, *J.*, dissenting from the denial of reh'g *en banc*); *id.* at 60 (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 65 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 59 (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 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 67–68 (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 68 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 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 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 64 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).

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.

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.

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 222.

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 75.

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 222. 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 223.

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 55 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 55 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 224.

8 *Id.* at 224.

9 Majority Op. at 203.

10 *Id.*

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 221. 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.*

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.*

18 *Id.*

19 The first step of the extraterritorial analysis is "to determine whether the relevant statutory provision contemplates extraterritorial application." Majority Op. at 210 (citing *Morrison*, 561 U.S. at 262–65, 130 S.Ct. 2869). 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 210–16, 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, 6 L.Ed. 111 (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 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, 107 S.Ct. 2542, 96 L.Ed.2d 461 (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 221 (emphasis added). Warrants protect privacy through the Fourth Amendment requirement that they issue only upon probable cause. *See* Concurring Op. at 206–08.
>
> 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 216–20.

22 *Id.* at 56. 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 56 (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 56 (quoting Majority Op. at 217–18). 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 57.

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 56 (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 56. 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, 130 S.Ct. 2869.

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 58 (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.

25 *Id.* at 217; *see* 18 U.S.C. §§ 2701–03.

26 18 U.S.C. § 2701.

27 Majority Op. at 220 (emphasis added).

28 18 U.S.C. § 2701.

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

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 214, 220. 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 220, 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).

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 60 (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 220. 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 56 (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 220. Naked assertions, however, do not the law make.

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.

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 60 (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 55 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.

1 On the panel's reasoning, if on September 10, 2001, the government had been able to show probable cause to believe that Mohamed Atta, Abdul Aziz al Omari, etc., were communicating electronically about an imminent, devastating attack on the United States, and that Microsoft possessed those emails, no federal court could have issued a § 2703(a) warrant compelling Microsoft to disclose those emails if it had stored them overseas, even though its employees would not have had to leave their desks in Redmond, Washington, to retrieve them.

2 *See* Restatement (Third) of Foreign Relations Law § 432(2) ("A state's law enforcement officers may exercise their functions in the territory of another state only with the consent of the other state, given by duly authorized officials of that state."); 1 *Oppenheim's International Law* § 119 (Robert Jennings & Arthur Watts, eds., 9th ed. 1992) ("It is ... a breach of international law for a state without permission to send its agents into the territory of another state to apprehend persons accused of having committed a crime."); *The Apollon*, 22 U.S. (9 Wheat.) 362, 371, 6 L.Ed. 111 (1824) (Story, J.) (holding that "[i]t would be monstrous to suppose that our revenue officers were authorized to enter into foreign ports and territories, for the purpose of seizing vessels which had offended against our laws" because such conduct would be "a clear violation of the laws of nations"); *The Nereide*, 13 U.S. (9 Cranch) 388, 423, 3 L.Ed. 769 (1815) (Marshall, C.J.) ("[T]he Court is bound by the law of nations which is a part of the law of the land.").

End of Document