GERARD E. LYNCH, *Circuit Judge*, concurring in the judgment:

I am in general agreement with the Court's conclusion that, in light of the presumption against extraterritorial application of congressional enactments, the Stored Communications Act ("SCA" or the "Act") should not, on the record made by the government below, be construed to require Microsoft to turn over records of the content of emails stored on servers in Ireland. I write separately to clarify what, in my view, is at stake and not at stake in this case; to explain why I believe that the government's arguments are stronger than the Court's opinion acknowledges; and to emphasize the need for congressional action to revise a badly outdated statute.

I

An undercurrent running through Microsoft's and several of its amici's briefing is the suggestion that this case involves a government threat to individual privacy. I do not believe that that is a fair characterization of the stakes in this dispute. To uphold the warrant here would not undermine basic values of privacy as defined in the Fourth Amendment and in the libertarian traditions of this country.

As the majority correctly points out, the SCA presents a tiered set of requirements for government access to electronic communications and information relating to them. Although Congress adopted the Act in order to provide some privacy protections to such communications, *see* H.R. Rep. No. 99-647, at 21–23 (1986); S. Rep. No. 99-541, at 3 (1986), those requirements are in many ways less protective of privacy than many might think appropriate. *See, e.g.*, *United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010) (holding that the SCA violates the Fourth Amendment to the extent that it allows government agents to obtain the contents of emails

without a warrant);[1] Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1214 (2004) (emphasizing that "[t]he SCA is not a catch-all statute designed to protect the privacy of stored Internet communications" and that "there are many problems of Internet privacy that the SCA does not address"). But this case does not require us to address those arguable defects in the statute. That is because in this case, the government complied with the most restrictive privacy-protecting requirements of the Act. Those requirements are consistent with the highest level of protection ordinarily required by the Fourth Amendment for the issuance of search warrants: a demonstration by the government to an independent judicial officer that evidence presented on oath justifies the conclusion that there is probable cause to believe that a crime has been committed, and that evidence of such crime can be found in the communications sought by the government.

That point bears significant emphasis. In this case, the government proved to the satisfaction of a judge that a reasonable person would believe that the records sought contained evidence of a crime. That is the showing that the framers of our Bill of Rights believed was sufficient to support the issuance of search warrants. U.S. Const. amend. IV ("[N]o Warrants shall issue, but upon probable cause . . . ."). In other words, in the ordinary domestic law enforcement context, if the government had made an equivalent showing that evidence of a crime could be found in a citizen's home, that showing would permit a judge to authorize law enforcement agents to forcibly enter that home and search every area of the home to locate the

[1] In the wake of *Warshak*, it has apparently been the policy of the Department of Justice since 2013 always to use warrants to require the disclosure of the contents of emails under the SCA, even when the statute permits lesser process. H.R. Rep. No. 114-528, at 9 (2016).

evidence in question, and even (if documentary or electronic evidence was sought) to rummage through file cabinets and to seize and examine the hard drives of computers or other electronic devices. That is because the Constitution protects "[t]he right of the people to be secure in their persons, houses, papers and effects" not absolutely, but only "against *unreasonable* searches and seizures," *id*. (emphasis added), and strikes the balance between the protection of privacy and the needs of law enforcement by requiring, in most cases, a warrant supported by a judicial finding of probable cause before the most intrusive of searches can take place. *See, e.g.*, *Riley v. California*, 134 S. Ct. 2473, 2482 (2014).

Congress, of course, is free to impose even stricter requirements on specific types of searches – and it has occasionally done so, for example in connection with the real-time interception of communications (as in wiretapping and electronic eavesdropping). *See* 18 U.S.C. § 2518(3)(a) (permitting the approval of wiretap applications only in connection with investigations of certain enumerated crimes); *id*. § 2518(3)(c) (requiring that a judge find that "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous" before a wiretap application can be approved). But it has not done so for permitting government access to any category of *stored* electronic communications, and Microsoft does not challenge the constitutional adequacy of the protections provided by the Act to those communications. Put another way, Microsoft does not argue here that, if the emails sought by the government were stored on a server at its headquarters in Redmond, Washington, there would be any constitutional obstacle to the government's acquiring them by the same means that it used in this case. Indeed, as explained above, the showing made by the government would support a warrant that permitted agents to forcibly enter those headquarters and seize the server itself.

I emphasize these points to clarify that Microsoft's argument is not that the government does not have sufficiently solid information, and sufficiently important interests, to justify invading the privacy of the customer whose emails are sought and acquiring records of the contents of those emails. Microsoft does not ask the Court to create, as a matter of constitutional law, stricter safeguards on the protection of those emails – and the Court does not do so. Rather, the sole issue involved is whether Microsoft can thwart the government's otherwise justified demand for the emails at issue by the simple expedient of choosing – in its own discretion – to store them on a server in another country.

That discretion raises another point about privacy. Under Microsoft's and the Court's interpretation of the SCA, the privacy of Microsoft's customers' emails is dependent not on the traditional constitutional safeguard of private communications – judicial oversight of the government's conduct of criminal investigations – but rather on the business decisions of a private corporation. The contract between Microsoft and its customers does not limit the company's freedom to store its customers' emails wherever it chooses, and if Microsoft chooses, for whatever reasons of profit or cost control, to repatriate the emails at issue here to a server in United States, there will be no obstacle to the government's obtaining them. As the Court points out, Microsoft does in fact choose to locate the records of anyone who *says* that he or she resides in the United States on domestic servers. It is only *foreign* customers, and those Americans who *say* that they reside abroad, who gain any enhanced protection from the Court's holding. And that protection is not merely enhanced, it is *absolute*: the government can never obtain a warrant that would require Microsoft to turn over those emails, however certain it may be that they

contain evidence of criminal activity, and even if that criminal activity is a terrorist plot.[2] Or to be more precise, the customer's privacy in that case is absolute *as against the government*; her privacy is protected against *Microsoft* only to the extent defined by the terms of her (adhesion) contract with the company.

Reasonable people might conclude that extremely stringent safeguards ought to apply to government investigators' acquisition of the contents of private email communications, and that the provisions of the SCA, as applied domestically, should be enhanced to provide even greater privacy, at an even higher cost to criminal investigations. Other reasonable people might conclude that, at least in some cases, investigators should have freer access to stored communications. It is the traditional task of Congress, in enacting legislation, and of the courts, in interpreting the Fourth Amendment, to strike a balance between privacy interests and law enforcement needs. But neither privacy interests nor the needs of law enforcement vary depending on whether a private company chooses to store records here or abroad – particularly when the "records" are electronic zeros and ones that can be moved around the world in seconds, and *will* be so moved whenever it suits the convenience or commercial purposes of the company. The issue facing the Court, then, is not actually about the need to enhance privacy protections for information that Americans choose to store in the "cloud."

---

[2] Although the Court does not reach the question, its opinion strongly suggests that that protection is absolute in the further sense that it applies also to less-protected categories of information otherwise reachable by the SCA's other disclosure-compelling instruments – subpoenas and court orders. If, as the Court holds, the "focus" of the SCA is privacy, and the relevant territorial locus of the privacy interest is where the customer's protected content is stored, *see* Majority Op. at 39, the use of the SCA to compel the disclosure of *any* email-related records stored abroad is impermissibly extraterritorial, regardless of the category of information or disclosure order.

II

In emphasizing the foregoing, I do not for a moment mean to suggest that this case is not important, or that significant non-privacy interests may not justify a congressional decision to distinguish records stored domestically from those stored abroad. It is important to recognize, however, that the dispute here is not about privacy, but rather about the international reach of American law. That question is important in its own right, and some further clarifications are in order about the division of responsibility between the courts and Congress in addressing it.

The courts have a significant role in the protection of privacy, because the Constitution sets limits on what even the elected representatives of the people can authorize when it comes to searches and seizures. Specifically, the courts have an independent responsibility to interpret the Fourth Amendment, an explicit check on Congress's power to authorize unreasonable searches. What searches are unreasonable is of course a difficult question, particularly when courts are assessing statutory authorizations of novel types of searches to deal with novel types of threat. In that context, courts need to be especially cautious, and respectful of the judgments of Congress. *See*, *e.g.*, *ACLU v. Clapper*, 785 F.3d 787, 824–25 (2d Cir. 2015). But it is ultimately the courts' responsibility to ensure that constitutional restraints on searches and seizures are respected.

Whether American law applies to conduct occurring abroad is a different type of question. That too is sometimes a difficult question. It will often be tempting to attempt to protect American interests by extending the reach of American law and undertaking to regulate conduct that occurs beyond our borders. But there are significant practical and policy limitations on the desirability of doing so. We live in a system of independent sovereign nations, in which other countries have their own ideas, sometimes at odds with ours, and their own legitimate

interests. The attempt to apply U.S. law to conduct occurring abroad can cause tensions with those other countries, most easily appreciated if we consider the likely American reaction if France or Ireland or Saudi Arabia or Russia proclaimed its right to regulate conduct by Americans within our borders.

But the decision about whether and when to apply U.S. law to actions occurring abroad is a question that is left entirely to Congress. *See Benz v. Compania Naviera Hidalgo, S.A.*, 353 U.S. 138, 147 (1957) (Congress "alone has the facilities necessary to make fairly [the] important policy decision" whether a statute applies extraterritorially). No provision of the Constitution limits Congress's power to apply its laws to Americans, or to foreigners, abroad, and Congress has on occasion done so, expressly or by clear implication. The courts' job is simply to do their best to understand what Congress intended. Where Congress has clearly indicated that a law applies extraterritorially, as for example in 18 U.S.C. § 2332(a), which prohibits the murder of U.S. citizens abroad, the courts apply the law as written. *See RJR Nabisco, Inc. v. European Cmty.*, 579 U.S. __, __, 2016 WL 3369423, at *9–10 (June 20, 2016). We do the same when a law clearly applies only domestically.

The latter situation is far more common, so common that it is the ordinary presumption. When Congress makes it a crime to "possess a controlled substance," 21 U.S.C. § 844(a), it does not say that it is a crime to possess dangerous or addictive drugs *in the United States*. It speaks absolutely, as if proclaiming a universal rule, but we understand that the law applies only here; it does not prohibit the possession of marijuana by a Dutchman, or even by an American, in the Netherlands. "Congress generally legislates with domestic concerns in mind," *RJR Nabisco*, 2016 WL 3369423, at *8, quoting *Smith v. United States*, 507 U.S. 197, 204 n.5 (1993), and so,

unless Congress clearly indicates to the contrary, we presume that statutes have only domestic effect.

I have little trouble agreeing with my colleagues that the SCA does not have extraterritorial effect. As the Supreme Court recently made clear in *RJR Nabisco*, the presumption applies not only to statutes that straightforwardly regulate or criminalize conduct, but also to jurisdictional, procedural and remedial statutes. *Id*. at *15–16; *see also Loginovskaya v. Batratchenko*, 764 F.3d 266, 272 (2d Cir. 2014) (rejecting the argument that the presumption "governs substantive (conduct-regulating) provisions rather than procedural provisions"). Moreover, *RJR Nabisco* also reemphasized that the relevant question is not whether we think Congress "would have wanted" the statute to apply extraterritorially had it foreseen the precise situation before us, but whether it made clear its intention to give the statute extraterritorial effect. *RJR Nabisco*, 2016 WL 3369423, at *7. There is no indication whatsoever in the text or legislative history that Congress intended the Act to have application beyond our borders. It would be quite surprising if it had. The statute was adopted in the early days of what is now the internet, when Congress could hardly have foreseen that multinational companies providing digital services of all sorts would one day store vast volumes of communications and other materials for ordinary people and easily be able to move those materials across borders at lightning speed. *See* Majority Op. at 14.

The tricky part, in a world of transnational transactions taking place in multiple jurisdictions at once, is deciding whether a proposed application of a statute is domestic or extraterritorial. That determination can be complicated even for criminal acts when they touch on multiple jurisdictions, but the problem is particularly acute when we deal not with a simple

effort to regulate behavior that – given the physical limitations of human bodies – can often be fixed to a specific location, but with statutes that operate in more complex fashions. If SCA warrants were traditional search warrants, permitting law enforcement agents to search a premises and seize physical objects, the extraterritoriality question would be relatively easy: a warrant authorizing a search of a building physically located in Ireland would plainly be an extraterritorial application of the statute (and it would be virtually inconceivable under ordinary notions of international law that Congress would ever attempt to authorize any such thing). But as the government points out, this case differs from that classic scenario with respect to both the nature of the legal instrument involved and the nature of the evidentiary material the government seeks.

First, the "warrant" required for the government to obtain the emails sought in this case does not appear to be a traditional search warrant. Significantly, the SCA does not describe the warrant as a *search* warrant. Nor does it contain language implying (let alone saying outright) that the warrant to which it refers authorizes government agents to go to the premises of a service provider without prior notice to the provider, search those premises until they find the computer, server or other device on which the sought communications reside, and seize that device (or duplicate and "seize" the relevant data it contains).[3] Rather, the statute expressly

[3] I do note, however, that the particular warrant in this case states that the government "requests the search of" a "PREMISES" and "COMMAND[S]" an officer to "execute" the warrant on or before a certain date and time. J.A. 44. Neither party argues that this case turns on the language in the warrant itself, and the government explains that this language was included only because the warrant "was prepared using the generic template for search warrants." Gov't Br. 20. Nevertheless, it is worth emphasizing that the government itself chose the "template" it used to create the warrant it then asked the magistrate judge to sign. It is, to say the least, unimaginative for the government to utilize a warrant form that purports to authorize conduct that the statute under which it is obtained plainly does not permit, and then to turn around and

requires the "warrant" not to authorize a search or seizure, but as the procedural mechanism to allow the government to "require a [service provider] to disclose the contents of [certain] electronic communication[s]" *without notice to the subscriber or customer*. 18 U.S.C. § 2703(b)(1)(A). Parallel provisions permit the government to require equivalent disclosure of the communications by the service provider by a simple administrative subpoena or by a court order, provided only that notice is provided to the subscriber. *Id*. § 2703(b)(1)(B).[4] Indeed, the various methods of obtaining the communications, with or without notice, are not merely parallel – they all depend on the same verbal phrase. They are simply alternative means, applicable in different circumstances, to "require [the service provider] to disclose [the communications]." *Id*. § 2703(a), (b).

---

argue that this sort of warrant is completely different from what its language tells us it is, and that the language is unimportant because the government simply used the same formal template it uses under other, more traditional circumstances involving physical searches.

[4] One category of communications – those held "in electronic storage" by an electronic communication service for one hundred and eighty days or less – is reachable only by SCA warrant, with or without notice to the customer. 18 U.S.C. § 2703(a). But, although we ourselves have not addressed the issue, the majority view is that, once the user of an entirely web-based email service (such as Microsoft's) opens an email he has received, that email is no longer "in electronic storage" on an electronic communication service. *See Lazette v. Kulmatycki*, 949 F. Supp. 2d 748, 758 (N.D. Ohio 2013); *Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965, 987 (C.D. Cal. 2010); *United States v. Weaver*, 636 F. Supp. 2d 769, 773 (C.D. Ill. 2009); *Jennings v. Jennings*, 736 S.E.2d 242, 245 (S.C. 2012); *id*. at 248 (Toal, C.J., concurring in the result); Kerr, *A User's Guide*, *supra*, at 1216–18 & n.61; *cf. Anzaldua v. Ne. Ambulance & Fire Prot. Dist.*, 793 F.3d 822, 840–42 (8th Cir. 2015) (message retained on Gmail server in "sent" folder was not in electronic storage). *But see Cheng v. Romo*, Civ. No. 11-10007-DJC, 2013 WL 6814691, at *3–5 (D. Mass. Dec. 20, 2013); *Pure Power Boot Camp v. Warrior Fitness Boot Camp*, 587 F. Supp. 2d 548, 555 (S.D.N.Y. 2008); *cf. Theofel v. Farey-Jones*, 359 F.3d 1066, 1075–77 (9th Cir. 2003) (message is in electronic storage until it "has expired in the normal course"). Under that reading of the statute, only emails that have not yet been opened by the recipient fall into the category described above.

This difference is significant if we are looking to determine the "focus" of the SCA for purposes of determining whether a particular application of the statute is or is not extraterritorial. *See Morrison v. Nat'l Australia Bank Ltd.*, 561 U.S. 247, 266–69 (2010). A search warrant "particularly describing the place to be searched, and the persons or things to be seized," U.S. Const. amend. IV, is naturally seen as focused on the *place* to be searched; as explained above, if the government argued that a statute authorized a search of a place outside the United States, that would clearly be an extraterritorial application of the statute. Here, however, the SCA warrant provision does not purport to authorize any such thing. Just like the parallel subpoena and court order provisions, it simply authorizes the government to *require the service provider to disclose* certain communications to which it has access.[5] The government quite reasonably argues that

[5] Although the Supreme Court has not addressed the question, there is considerable case law, including in this circuit, permitting the exercise of subpoena powers in precisely the situation in which the government demands records located abroad from an American company, or a foreign company doing business here. *See, e.g.*, *Linde v. Arab Bank, PLC*, 706 F.3d 92 (2d Cir. 2013); *United States v. Bank of Nova Scotia*, 740 F.2d 817 (11th Cir. 1984); *Marc Rich & Co., A.G. v. United States*, 707 F.2d 663 (2d Cir. 1983); *United States v. First Nat'l City Bank*, 396 F.2d 897, 900–01 (2d Cir. 1968) ("It is no longer open to doubt that a federal court has the power to require the production of documents located in foreign countries if the court has in personam jurisdiction of the person in possession or control of the material."). At least as far as American courts are concerned (some foreign governments may think otherwise), such demands for the production of records are not seen as categorically impermissible extraterritorial uses of American investigatory powers, in the way that search warrants for foreign locations certainly would be. *Compare* Restatement (Third) of Foreign Relations Law § 442(1)(a) ("A court or agency in the United States, when authorized by statute or rule of court, may order a person subject to its jurisdiction to produce documents, objects, or other information relevant to an action or investigation, even if the information or the person in possession of the information is outside the United States.") *with id.* § 433(1) ("Law enforcement officers of the United States may exercise their functions in the territory of another state only (a) with the consent of the other state and if duly authorized by the United States; and (b) in compliance with the laws both of the United States and of the other state.").

Microsoft attempts to distinguish the cases cited above on the ground that the subpoenas in those cases required their recipients to disclose only the contents of their own business records, and not the records of a third party "held in trust" by the recipients. Appellant's Br. 48.

the focus of such a provision is not on the place where the service provider stores the communications, but on the place where the service provider discloses the information to the government, as requested.[6]

The nature of the records demanded is also relevantly different from that of the physical documents sought by traditional search warrants. Tangible documents, having a material existence in the physical world, are stored in a particular physical location. Executing a traditional search warrant requires a visit to that location, to visually inspect the documents to select the responsive materials and to take those materials away. Even when tangible documents are sought by subpoena, rather than by search warrant, it is arguable that the focus of the

---

"Email correspondance," Microsoft explains, is unlike bank records because it "is personal, even intimate," and "can contain the sum of an individual's private life." *Id*. at 44 (internal quotation marks omitted). Even assuming, however, that Microsoft accurately characterizes the cases it seeks to distinguish, *but cf. In re Horowitz*, 482 F.2d 72 (2d Cir. 1973) (partially upholding a subpoena requiring an accountant to produce the contents of three locked file cabinets belonging to a client), this privacy-based argument is, as explained above, a red herring. Microsoft does not dispute that the government could have required the disclosure of the emails at issue here if they were stored in the United States, and Microsoft's decision to store them abroad does not obviously entitle their owner to any higher degree of privacy protection.

[6] As the government notes, the selection of the term "warrant" to describe an instrument that does not operate like a traditional arrest or search warrant is easily explained by the fact that the provision in question, which permits government access to a person's stored communications without notice to that person, provides the highest level of privacy protection in the statute: the requirement that an independent judicial officer determine that probable cause exists to believe that a crime has been committed and that evidence of that crime may be found in the communications demanded. The *showing* necessary to obtain judicial authorization to require the service provider to disclose the communications is that associated with traditional warrants; the *manner* in which the disclosure is obtained by the government, however, is more closely analogous to the workings of subpoenas and court-ordered discovery: the government serves the service provider with an order from a court that requires the *service provider* to look within its records and *disclose* the specified information to the government; it does not present to the service provider a court order that permits *government agents* to search through the service provider's premises and documents and *seize* the specified information.

subpoena, for extraterritoriality purposes, is on the place where the documents are stored, since in order to comply with a subpoena seeking documents stored abroad, corporate employees will have to be present in the foreign location where the documents exist to inspect and select the relevant documents, which will then have to be transported out of that location and into the United States.

Electronic "documents," however, are different. Their location on a computer server in a foreign country is, in important ways, merely virtual. *See* Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. Pa. L. Rev. 373, 408 (2014) (explaining that "the very idea of online data being located in a particular physical 'place' is becoming rapidly outdated," because computer files can be fragmented and dispersed across many servers). Corporate employees in the United States can review those records, when responding to the "warrant" or subpoena or court order just as they can do in the ordinary course of business, and provide the relevant materials to the demanding government agency, without ever leaving their desks in the United States. The entire process of compliance takes place domestically.

The government's characterization of the warrant at issue as domestic, rather than extraterritorial, is thus far from frivolous, and renders this, for me, a very close case to the extent that the presumption against extraterritoriality shapes our interpretation of the statute. One additional potential fact heightens the complexity. We do not know, on this record, whether the customer whose emails were sought by the government is or is not a United States citizen or resident. It is not clear that whether the customer is a United States person or not matters to the rather simplistic "focus" test adopted by the Supreme Court in *Morrison*, although it would have mattered to the more flexible test utilized by the Second Circuit in that case. *See Morrison v.*

Nat'l Australia Bank Ltd., 547 F.3d 167, 171 (2d Cir. 2008). But it seems to me that it *should* matter. The Supreme Court has rightly pointed out that the presumption against extraterritoriality is more than simply a means for avoiding conflict with foreign laws. *See Morrison*, 561 U.S. at 255. At the same time, the presumption that Congress legislates with domestic concerns pre-eminent in its collective mind does not fully answer the question what those domestic concerns are in any given case. *See id.* at 266. Particularly in connection with statutes that provide tools to law enforcement, one imagines that Congress is concerned with balancing liberty interests of various kinds against the need to enforce *domestic* law. Thus, when Congress authorizes the (American) government to obtain access to certain information, one might imagine that its focus is on balancing the liberty interests of *Americans* (and of other persons residing in the U.S.) against the need to enforce *American* laws. Congress might also reasonably be concerned about the diplomatic consequences of over-extending the reach of American law enforcement officials. This suggests a more complex balancing exercise than identifying a single "focus" of the legislation, the latter approach being better suited to determining whether given *conduct* fitting within the literal words of a prohibition should be characterized as domestic or extraterritorial.[7]

---

[7] While, for these reasons, it may be impossible to answer satisfactorily the question what the single focus of the SCA is, I note that I have considerable doubts about the answer supplied by the Court, which holds that the SCA provisions at issue here "focus on protecting the privacy of the content of a user's stored electronic communications." Majority Op. at 33. Privacy, however, is an abstract concept with no obvious territorial locus; the conclusion that the SCA's focus is privacy thus does not really help us to distinguish domestic applications of the statute from extraterritorial ones. "The real motor of the Court's opinion," *Morrison*, 561 U.S. at 284 (Stevens, *J.*, concurring in the judgment), then, is less the conclusion that the statute focuses on privacy than the majority's further determination that the locus of the invasion of privacy is where the private content is stored – a determination that seems to me suspect when the content consists of emails stored in the "cloud." It seems at least equally persuasive that the invasion of privacy occurs where the person whose privacy is invaded customarily resides.

Because Microsoft relies solely on customers' self-reporting in classifying customers by residence, and stores emails (but only for the most part, and only in the interests of efficiency and good customer service) on local servers – and because the government did not include in its warrant application such information, if any, as it had about the target of its investigation – we do not know the nationality of the customer. If he or she is Irish (as for all we know the customer is), the case might present a troubling prospect from an international perspective: the Irish government and the European Union would have a considerable grievance if the United States sought to obtain the emails of an Irish national, stored in Ireland, from an American company which had marketed its services to Irish customers in Ireland. The case looks rather different, however – at least to me, and I would hope to the people and officials of Ireland and the E.U. – if the American government is demanding from an American company emails of an American citizen resident in the U.S., which are accessible at the push of a button in Redmond, Washington, and which are stored on a server in Ireland only as a result of the American customer's misrepresenting his or her residence, for the purpose of facilitating domestic violations of American law, by exploiting a policy of the American company that exists solely for reasons of convenience and that could be changed, either in general or as applied to the particular customer, at the whim of the American company. Given that the extraterritoriality inquiry is essentially an effort to capture the congressional will, it seems to me that it would be remarkably formalistic to classify such a demand as an extraterritorial application of what is effectively the subpoena power of an American court.

These considerations give me considerable pause about treating SCA warrants as extraterritorial whenever the service provider from whom the government seeks to require

production has chosen to store the communications on a server located outside the United States. Despite that hesitation, however, I conclude that my colleagues have ultimately reached the correct result. If we frame the question as whether Congress has demonstrated a clear intention to reach situations of this kind in enacting the Act, I think the better answer is that it has not, especially in the case (which could well be this one) of records stored at the behest of a foreign national on servers in his own country. The use of the word "warrant" may not compel the conclusion that Congress intended to reach only domestically-stored communications that could be reached by a conventional search warrant, because, for the reasons given above, that label should not be controlling. *Cf. Big Ridge, Inc. v. Fed. Mine Safety & Health Review Comm'n*, 715 F.3d 631, 645–46 (7th Cir. 2013) (explaining that "we look to the substance of [the government's] inspection power rather than how the Act nominally refers to those powers," and holding that document requests under the Mine Safety and Health Act of 1977 should be treated as administrative subpoenas rather than as a search or seizure). But it is hard to believe that Congress would have used such a loaded term, and incorporated by reference the procedures applicable to purely domestic warrants, if it had given any thought at all to potential transnational applications of the statute. Nor is it likely that Congress contemplated such applications for a single moment. The now-familiar idea of "cloud" storage of personal electronic data by multinational companies was hardly foreseeable to Congress in 1986, and the related prospects for diplomatic strife and implications for American businesses operating on an international scale were surely not on the congressional radar screen when the Act was adopted. We should not lightly assume that Congress chose to permit SCA warrants for communications stored abroad when there is no sign that it considered the consequences of doing so. *See Kiobel*

v. Royal Dutch Petroleum Co., 133 S. Ct. 1659, 1664 (2013) ("The presumption against extraterritorial application helps ensure that the Judiciary does not erroneously adopt an interpretation of U.S. law that carries foreign policy consequences not clearly intended by the political branches."). Thus, while I think the case is closer – and the government's arguments more potent – than is reflected in the Court's opinion, I come out in the same place.

III

Despite ultimately agreeing with the result in this case, I dwell on the reasons for thinking it close because the policy concerns raised by the government are significant, and require the attention of Congress. I do not urge that Congress write the government's interpretation into the Act. That is a policy judgment on which my own views have no particular persuasive force. My point is simply that the main reason that both the majority and I decide this case against the government is that there is no evidence that Congress has *ever* weighed the costs and benefits of authorizing court orders of the sort at issue in this case. The SCA became law at a time when there was no reason to do so. But there is reason now, and it is up to Congress to decide whether the benefits of permitting subpoena-like orders of the kind issued here outweigh the costs of doing so.

Moreover, while I do not pretend to the expertise necessary to advocate a particular answer to that question, it does seem to me likely that a sensible answer will be more nuanced than the position advanced by either party to this case. As indicated above, I am skeptical of the conclusion that the mere location abroad of the server on which the service provider has chosen to store communications should be controlling, putting those communications beyond the reach of a purely "domestic" statute. That may be the default position to which a court must revert in

the absence of guidance from Congress, but it is not likely to constitute the ideal balance of conflicting policy goals. Nor is it likely that the ideal balance would allow the government free rein to demand communications, wherever located, from any service provider, of whatever nationality, relating to any customer, whatever his or her citizenship or residence, whenever it can establish probable cause to believe that those communications contain evidence of a violation of American criminal law, of whatever degree of seriousness. Courts interpreting statutes that manifestly do not address these issues cannot easily create nuanced rules: the statute either applies extraterritorially or it does not; the particular demand made by the government either should or should not be characterized as extraterritorial. Our decision today is thus ultimately the application of a default rule of statutory interpretation to a statute that does not provide an explicit answer to the question before us. It does not purport to decide what the answer should be, let alone to impose constitutional limitations on the range of solutions Congress could consider.

Congress need not make an all-or-nothing choice. It is free to decide, for example, to set different rules for access to communications stored abroad depending on the nationality of the subscriber or of the corporate service provider. It could provide for access to such information only on a more demanding showing than probable cause, or only (as with wiretapping) where other means of investigation are inadequate, or only in connection with investigations into extremely serious crimes rather than in every law enforcement context. Or it could adopt other, more creative solutions that go beyond the possibilities evident to federal judges limited by their own experience and by the information provided by litigants in a particular case.

In addition, Congress need not limit itself to addressing the particular question raised by this case. The SCA was adopted in 1986, at a time when the kinds of services provided by "remote computing services" were not remotely as extensive and complex as those provided today, and when the economic and security concerns presented by such services were not remotely as important as they are now. More than a dozen years ago, a leading commentator was expressing the need to reform the Act. *See* Kerr, *A User's Guide*, *supra*, at 1233–42. It would seem to make sense to revisit, among other aspects of the statute, whether various distinctions, such as those between communications stored within the last 180 days and those that have been held longer, between electronic communication services and remote computing services, or between disclosures sought with or without notice to the customer, should be given the degree of significance that the Act accords them in determining the level of privacy protection it provides, or whether other factors should play some role in that determination.[8]

Congress has, in the past, proven adept at adopting rules for adapting the basic requirements of the Fourth Amendment to new technologies. The wiretapping provisions of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510–22, for example, proved to be a remarkably stable and effective structure for dealing with the privacy and law enforcement issues raised by electronic surveillance in the telephone era. More recently,

[8] As the Court notes, Majority Op. at 28 n.23, the House of Representatives recently passed a bill amending the SCA's required disclosure provisions. Email Privacy Act, H.R. 699, 114th Cong. § 3 (2016). That bill would require the government to obtain a warrant before it can compel the disclosure of the contents of any electronic communication "stored, held, or maintained" by either an electronic communication service or (under certain circumstances) a remote computing service, no matter the length of the period of storage. *Id*. It does not, however, address those provisions' extraterritorial reach or significantly modernize the statute's structure. *See* Kerr, *The Next Generation*, *supra*, at 386–89 (criticizing a proposal similar to the Email Privacy Act for "work[ing] within [the SCA's] outdated framework"). As of this writing, the Senate has not taken any action on the bill.

Congress was able to address the concerns presented by the mass acquisition of metadata by the National Security Agency by creating a more nuanced statute than that which the NSA had claimed as authority for its actions. *See ACLU v. Clapper*, 804 F.3d 617, 620 (2d Cir. 2015), discussing the USA FREEDOM Act of 2015, Pub. L. No. 114-23, 129 Stat. 268 (2015). I fully expect that the Justice Department will respond to this decision by seeking legislation to overrule it. If it does so, Congress would do well to take the occasion to address thoughtfully and dispassionately the suitability of many of the statute's provisions to serving contemporary needs. Although I believe that we have reached the correct result as a matter of interpreting the statute before us, I believe even more strongly that the statute should be revised, with a view to maintaining and strengthening the Act's privacy protections, rationalizing and modernizing the provisions permitting law enforcement access to stored electronic communications and other data where compelling interests warrant it, and clarifying the international reach of those provisions after carefully balancing the needs of law enforcement (particularly in investigations addressing the most serious kinds of transnational crime) against the interests of other sovereign nations.

* * *

For these reasons, I concur in the result, but without any illusion that the result should even be regarded as a rational policy outcome, let alone celebrated as a milestone in protecting privacy.