No. 17-2

IN THE

Supreme Court of the United States

UNITED STATES OF AMERICA,
Petitioner,
v.
MICROSOFT CORPORATION,
Respondent.

On Writ of Certiorari to the United States Court of Appeals for the Second Circuit

BRIEF FOR THE COMPETITIVE ENTERPRISE INSTITUTE, CATO INSTITUTE, TECHFREEDOM, REASON FOUNDATION, AND AMERICAN CONSUMER INSTITUTE CENTER FOR CITIZEN RESEARCH AS *AMICI CURIAE* IN SUPPORT OF RESPONDENT

Ilya Shapiro
Trevor Burrus
Reilly Stephens
CATO INSTITUTE
1000 Mass. Ave. N.W.
Washington, D.C. 20001
(202) 842-0200
ishapiro@cato.org

Jim Harper
Counsel of Record
COMPETITIVE ENTERPRISE INSTITUTE
1310 L St. NW, 7th Floor
Washington, D.C. 20005
(202) 331-1010
jim.harper@cei.org

January 17, 2018

Additional counsel listed on inside cover

Berin Szóka
TECHFREEDOM
110 Maryland Ave. N.E.
Suite 409
Washington, D.C. 20002
(202) 803-2867
bszoka@techfreedom.org

Manuel S. Klausner
LAW OFFICES OF MANUEL S. KLAUSNER
One Bunker Hill Building
601 W. Fifth St.,
Suite 800
Los Angeles, CA 90071
(213) 617-0414
mklausner@klausnerlaw.us

QUESTION PRESENTED

Whether the warrant procedure established by 18 U.S.C. § 2703 can require a U.S. provider of email services to retrieve its customer's communications data from overseas for disclosure to the U.S. government.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

INTERESTS OF *AMICI CURIAE*[1]

The **Competitive Enterprise Institute** ("CEI") is a non-profit public policy organization dedicated to advancing the principles of limited government, free enterprise, and individual liberty. CEI publishes research and commentary on topics at the intersection of property rights, markets, free enterprise, and liberty.

The **Cato Institute** is a nonpartisan public policy research foundation dedicated to advancing the principles of individual liberty, free markets, and limited government. Cato's Robert A. Levy Center for Constitutional Studies promotes the principles of limited constitutional government that are the foundation of liberty. To those ends, Cato publishes books and studies, conducts conferences, produces the annual *Cato Supreme Court Review*, and files *amicus* briefs.

TechFreedom is a non-profit, non-partisan think tank dedicated to educating policymakers, the media, and the public about technology policy. TechFreedom defends the freedoms that make technological progress both possible and beneficial, including the privacy rights protected by federal legislation and the Fourth Amendment, the crown jewel of American civil liberties.

Reason Foundation is a nonpartisan, nonprofit think tank whose mission is to advance a free society through libertarian principles and policies—including free markets, individual liberty, and the rule of law. Reason supports dynamic market-based public policies that allow and encourage individuals and voluntary

---

[1] All parties lodged blanket consents with the Clerk. No counsel for any party authored this brief in whole or in part and no person or entity other than *amici* funded its preparation or submission.

institutions to flourish. Reason advances its mission by publishing Reason magazine, as well as public policy research and commentary on its websites. To further Reason's commitment to "Free Minds and Free Markets," it participates as *amicus* in cases raising constitutional issues.

The **American Consumer Institute Center for Citizen Research** ("ACI") is a 501(c)(3) nonprofit educational and research organization with a mission to identify, analyze, and protect the interests of consumers on various topics involving public policy, legislation, government regulation, and market competition and performance. ACI's work includes publishing and conducting extensive research on technology and consumer privacy issues.

This case concerns *amici* because it represents an opportunity to clarify and improve legal recognition of digital documents and protections therefor. *Amici* are particularly concerned with the erosion of legal protections for private data given changes in modern business practices and rapid technological advances. Proper administration of the Fourth Amendment and federal statutes would allow businesses to protect their customers' privacy consistent with their interests as determined in the marketplace.

INTRODUCTION AND SUMMARY OF ARGUMENT

This Court can reach the right decision and do so the right way by giving careful legal characterization to all the circumstances in this case. That is a challenge—and the case is before this Court—because digital materials and contexts interact slightly differently with otherwise familiar law and legislation.

This case has developed with little, if any, consideration of the legal interests of Microsoft customers. Those interests are established by privacy policies and Terms of Service documents. Microsoft provides its services subject to promises that allocate property rights in the data and communications produced during and by the use of the services. Microsoft maintains some rights to use data and the right to possess it, while the customer holds most rights to exclude others, to use the data, to sell it, and so on.

Awareness of the customer's property interest helps clarify that the mandatory information collection process established by the Stored Communications Act ("SCA") is properly conceived of as a warrant. Congress correctly characterized it as such.

Although historical practice and legal precedents are not a model of clarity, warrants and subpoenas occupy different spheres of compelled disclosure, distinguished by the opportunity of the interested party to contest the procedure. A subpoena asks the interested party for his or her own materials (or presence) and thus naturally provides him or her the opportunity to object before disclosure. A warrant is required when a similar process is executed without the knowledge—or over the contemporaneous objection—of the person affected. The warrant requirement appropriately controls misuse of that process.

Both the SCA and the Constitution require the approval of a neutral magistrate when law enforcement seeks customer communications from service providers such as Microsoft. But in other realms over the last century, administrative business practices and digitization have confused subpoena and warrant practice. Many more materials have moved into the hands of

third-party service providers, which have become repositories of documents and information in which their customers maintain acute personal and real legal interests. The "third-party subpoena" now allows government agents access to private information in amounts that would have been beyond the Framers' imagination and that would have required a warrant to amass in their time.

To rationalize what has happened in this case, the Court should recognize that, in the digital context, possession is often separate from other property rights, such as the right to exclude. That right is "one of the most essential sticks in the bundle of rights that are commonly characterized as property." *Kaiser Aetna v. United States*, 444 U.S. 164, 176 (1979); *see also Dolan v. City of Tigard*, 512 U.S. 374, 384 (1994); *Lucas v. South Carolina Coastal Council*, 505 U.S. 1003, 1044 (1992); *Nollan v. Calif. Coastal Comm'n*, 483 U.S. 825, 831 (1987). This Court can and should help refine the subpoena and warrant categories by acknowledging the property interests people maintain in digital materials that they don't always or necessarily possess.

Precise understanding of the technology and interests at stake also makes clear that an SCA order to retrieve data from an overseas server is extraterritorial. Just as an order to throw a rock over the Canadian border produces a result in Canada, an SCA warrant related to overseas data produces extraterritorial results. In terms of the statute's "focus," an SCA warrant order affects the Microsoft customer's privacy at the location and time of the copying, because his or her right to exclude others is compromised when the copy is made and sent. If the SCA's "focus" is regarded as

disclosure, the warrant affects the stored communications at the location and at the time of copying because the warrant is an essential step in the process of disclosing. In other words, regardless of how the larger doctrines apply, an SCA warrant aimed at overseas data is extraterritorial.

One might argue that, because contracts for digital communications services typically do allow information sharing in response to valid legal processes, they do not allocate a property interest to the customer when legal processes such as the SCA's are invoked. But the only way to give meaning to all contract terms is by reading them as requiring processes to have legal validity, not just adherence to legal or legislative formalities.

Another narrow argument is that denying the SCA extraterritorial reach would allow service providers to place data offshore for illegitimate purposes, such as to assist a criminal or criminal enterprise in evading U.S. law. Such an agreement would likely violate the law itself and be voided as contrary to public policy, a classic black-letter contracts concept. The beneficiary of the arrangement could not enjoy the property rights purportedly created by it, and the information could be retrieved without a warrant.

In sum, by knitting the modern digital context together with timeless principles of Anglo-American law, this Court can reach a decision that: (1) maintains continuity in the law and legal expectations, (2) avoids line-drawing and policymaking, (3) eschews inventing or extending doctrines without foundation in statutory language or constitutional text, and (4) provides justice to the parties. Crucially, the Court can provide

lower courts with the tools they need to fuse existing law to the burgeoning digital environment.

ARGUMENT

I. CONTRACTS ALLOCATE PROPERTY RIGHTS IN COMMUNICATIONS AND DATA

Microsoft provides services to its customers subject to promises that allocate property rights in the data and communications produced during and by the use of the services. Tracking how property concepts apply in this area helps delineate the framework in which the questions before this Court become easier to answer.

A. The MSN.com Privacy Policy Gives the Bulk of Data Ownership to the Customer

Consumer-facing digital businesses enter into very detailed arrangements with customers that divide up ownership of data used in the service and produced by use of the services. Microsoft's terms of service are no exception. They allocate the bulk of rights to control and use personal data to customers, consistent with practice across digital services. These property rights in data include the right of users to exclude others from personal data in all but closely defined circumstances.

The MSN.com privacy policy in effect as of August 2013 is typical in that it denies Microsoft rights to sell or share data, subject to specific exceptions.[2] "Except

[2] The document we rely on is reproduced on a site called Docracy, whose Terms of Service Tracker project "tracks changes to terms of service and privacy policy documents of many of the world's top websites." Probably due to a change in the URL structure of the

as described in this statement, we will not disclose your personal information outside of Microsoft and its controlled subsidiaries and affiliates without your consent." MSN.com Privacy Policy, Aug. 2013 snapshot, http://bit.ly/2AOzhwJ [hereinafter "2013 Microsoft Contract"]. Microsoft's current "privacy statement" includes a similar general statement limiting what it can share outside of Microsoft. "We share your personal data with your consent or as necessary to complete any transaction or provide and product you have requested or authorized." Microsoft Privacy Statement, http://bit.ly/2B6Z4R2 [hereinafter "2018 Microsoft Contract"]. Such language leaves the general right to exclude all others from the data with the customer. The possessive pronoun "your" signifies that the bulk of the ownership of the data is the customer's. *See also* Brief of The States of Vermont et al. as Amici Curiae at 4 (referring to companies as controlling "their customers' data").

Both policies include exceptions for sharing with law enforcement under specified circumstances. "We may access or disclose information about you, including the content of your communications, in order to: … comply with the law or respond to lawful requests or legal process." 2013 Microsoft Contract. "[W]e will access, transfer, disclose, and preserve personal data … when we have a good faith belief that doing so is necessary to: … comply with applicable law or respond to valid legal process, including from law enforcement or other government agencies." Microsoft 2018 Contract. As

---

MSN.com site, we could not find a version of this document at archive.org.

discussed below, these contract terms necessarily imply that any such process must be legally valid.

B. Contract Law, Federal Agency Enforcement, and Common Law Conversion All Accord with Data's Treatment as Property

Contract terms limiting access to personal information have a long history. *See, e.g., Peterson v. Idaho First Nat'l Bank*, 367 P.2d 284, 290 (Idaho 1961), *quoting* 7 Am. Jur., Banks, § 196 ("[I]t is an implied term of the contract between a banker and his customer that the banker will not divulge to third persons . . . either the state of the customer's account or any of his transactions with the bank, or any information relating to the customer acquired through the keeping of his account, unless the banker is compelled to do so by order of a court, [or] the circumstances give rise to a public duty of disclosure").

In the modern era, much enforcement of these rights is by government agencies standing in for consumers. *See, e.g.*, Federal Trade Comm'n, "Enforcing Privacy Promises" webpage, http://bit.ly/2B9ndGF. But there is also active litigation that asserts violation of contracts pertaining to terms of service, privacy policies, and the like. *See, e.g., In re Facebook Internet Tracking Litigation*, No. 5:12-md-02314-EJD (N.D. Cal. filed Feb. 8, 2012). These rights are property rights. *See U.S. Trust Co. v. New Jersey*, 431 U.S. 1, 19 n.16 (1977) ("Contract rights are a form of property"). There is no juridical way to characterize the exchange of promises between Microsoft and its customers other than as contracts allocating property rights.

Data are increasingly recognized as subject to conversion claims in state courts. In a leading case, *Thyroff v. Nationwide Mut. Ins. Co.*, 8 N.Y.3d 283 (N.Y. 2007), for example, the Second Circuit certified to the New York Court of Appeals this question: "Is a claim for the conversion of electronic data cognizable under New York law?" *Id.* at 285-86. The court responded affirmatively: electronic records maintained on a computer are "subject to claim of conversion in New York." *Id.* at 293.

Conversion of rights to data is also an available claim in Maryland and Massachusetts. *Thompson v. UBS Fin. Servs., Inc.*, 443 Md. 47, 58-59 (2015) ("[F]or conversion's purposes, there is no distinction between hard copy and electronic data, as long as a document, either paper or digital, embodies the plaintiff's right to the plaintiff's intangible property." (citations and quotations omitted); *Network Sys. Architects Corp. v. Dimitruk*, 23 Mass. L. Rep. 339 (2007) ("In the modern world, computer files hold the same place as physical documents have in the past. If paper documents can be converted, as they no doubt can, no reason appears that computer files cannot." (citations omitted)).

Conversion, of course, works slightly differently in the digital environment. When a digital item is taken, it is often a copy, and the original is left intact. Thus, the victim retains the ability to use the data. This has caused a division in North Carolina, where one court has denied a conversion claim, *see, e.g.*, *Addison Whitney, LLC v. Cashion*, 2017 NCBC LEXIS 51 *16-17, while another has upheld it, *Bridgetree, Inc. v. Red F Mktg. LLC*, No. 3:10-cv-00228-FDW-DSC, 2013 U.S. Dist. LEXIS 15372, at *49-50 (W.D.N.C. Feb. 5, 2013)

("Defendants' conduct did not need to completely deprive Plaintiff use and access to its computer files. It would be sufficient if Defendants' conduct violated Plaintiff's dominion or control over the property (here, the computer files), or if Defendants altered the condition of Plaintiff's rights to those computer files." (citations omitted)).

The Arkansas Supreme Court concludes that 'intangible property, such as electronic data . . . can be converted if the actions of the defendant are in denial of or inconsistent with the rights of the owner or person entitled to possession." *Integrated Direct Mktg., LLC v. Drew May & Merkle, Inc.*, 2016 Ark. 281, ¶ 6, 495 S.W.3d 73, 76.

Data is commonly and increasingly recognized as property for purposes of contract and conversion. Microsoft offers its services to the public subject to contracts that allocate property rights in data produced during, and by, the use of the services.

Data's status as property and its ownership in this case helps frame the issues before the Court. It helps make clear that the compelled disclosure the government seeks in this case is pursuant to a warrant, not a subpoena, and also why that is important.

II. THE GOVERNMENT SERVED A WARRANT ON MICROSOFT, NOT A SUBPOENA, AND THE DIFFERENCE IS IMPORTANT

In the court below, the government and Microsoft sparred over whether the process created by the SCA is a "warrant" or some other form of "compelled disclosure." Pet. App. 3a. That court concluded that the process at issue was, indeed, a warrant. *Id.* at 4a. "Warrant" is the terminology that Congress used, 18 U.S.C.

§ 2703, and it is correct. At first blush, it may seem like mere semantics, but there are important distinctions between warrants and subpoenas that the Court should highlight and clarify.

A. Changes in Technology and Business Have Collapsed Important Distinctions Between Subpoenas and Warrants That the Court Should Restore

The subpoena and the warrant arose very differently in history and have traditionally served very different roles in the administration of justice. "An order, usually in the form of a subpoena, directly commanded a subject—for example, requiring him to appear, testify, or produce his papers. . . . In contrast to a subpoena, a warrant was not an order to a subject, but to an officer to constrain a subject." Philip Hamburger, *Is Administrative Law Unlawful?* 176 (2014). Changes in technology and business practices are coupling with insufficient recognition of property rights in digital materials to threaten the collapse of the distinctions between subpoenas and warrants, and thus erode the protections of the Fourth Amendment.

At the time of the founding, neither the technology nor the business practices existed to produce third-party record-keeping that could reveal vast swaths of private and sensitive information. Persons, papers, houses, and effects generally hung together. With rare exceptions for the wealthy who traveled, the sensitive information and materials that merit constitutional protection rarely left the enclave of the home or proximity to the individual. *But see Ex Parte Jackson*, 96 U.S. 727, 733 (1878) (Fourth Amendment protection for sealed postal mail).

Thus, the two disclosure processes of the warrant and subpoena worked in tandem to administer disclosure of information to government investigators under conditions meant also to appropriately protect privacy. A subpoena—asking a person for his or her own testimony or things—inherently gave notice and thus the opportunity for pre-enforcement review should the recipient object. This Court recently reaffirmed the opportunity for pre-compliance review as integral to subpoenas. *City of Los Angeles v. Patel*, 135 S. Ct. 2443, 2451 (2015). A warrant, by contrast, was executed in secret or despite the contemporaneous objection of the subject of investigation. This required the advance approval of a neutral magistrate.

Law professor Christopher Slobogin has documented how shifting circumstances have collapsed the categories, allowing the "third-party subpoena" to eclipse the warrant as a tool for gathering personal information about criminal suspects while derogating the protections of the Fourth Amendment. Christopher Slobogin, *Subpoenas and Privacy*, 54 DePaul L. Rev. 805 (2005).

> At the end of the nineteenth century, *Boyd* [*v. United States*, 116 U.S. 616 (1886),] affirmed the common law ban on government efforts to obtain incriminating papers from their owners. Although that ban was soon lifted for business papers, only in the last quarter of the twentieth century did the Court relax constitutional strictures on subpoenas for self-incriminating personal papers. In contrast, constitutional restrictions on subpoenas for papers in the possession of third parties have always been lax. The historical change in this setting has not

> been in the law, but in the extent to which personal information is now housed with third parties.
>
> The end result of these developments is that, as a constitutional matter, the minimal relevance standard once used primarily in connection with business subpoenas now authorizes access to vast amounts of personal information, to wit, *any* personal information that is in record form, with the possible exception of information found in records possessed by the target that the government is not sure exist.

Id. at 826.

This Court's decision in *United States v. Miller*, 425 U.S. 435 (1976), is a leading illustration of how the "third-party subpoena" now allows government agents to access personal and private financial papers and information in quantities that would have been beyond contemplation at the time of the Framing. *Cf. United States v. Jones*, 132 S. Ct. 945, 950 (2012) (majority op.) ("we must 'assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'" quoting *Kyllo v. United States*, 533 U.S. 27, 34 (2001); *Id.* at 958 (Alito, J., concurring in judgment) (same language).

Miller's rationale has been extended to records of consumers' telephone calling, *Smith v. Maryland*, 442 U.S. 735 (1979); loan applications, *United States v. Payner*, 447 U.S. 727 (1980); personal records at medical institutions, *Webb v. Goldstein*, 117 F. Supp. 2d 289 (E.D.N.Y. 2000); *State v. Guido*, 698 A.2d 729 (R.I. 1997); *Corpus v. State*, 931 S.W.2d 30 (Tex. App. 1996); records held by auditors and accountants, *Wang v.*

United States, 947 F.2d 1400, 1403 (9th Cir. 1991); records of trustees in bankruptcy, *In re Lufkin*, 255 B.R. 204, 211 (Bankr. E.D. Tenn. 2000); and records held by the Veterans Administration. *Doe v. DiGenova*, 642 F. Supp. 624 (D.D.C. 1986).

Miller is distinguishable from this case because the *Miller* Court did not decide whether an individual may assert an interest in data when contract makes it or its contents items of property owned in relevant part by the person under investigation. Miller's counsel arguably relied solely on "reasonable expectation of privacy" doctrine in oral argument, and the decision characterized his argument as having that focus alone. *Miller*, 425 U.S. at 442 ("Respondent urges that he has a Fourth Amendment interest in the records kept by the banks because they are merely copies of personal records . . . in which he has a reasonable expectation of privacy. He relies on this Court's statement in *Katz v. United States*, 389 U.S. 347, 353 (1967)."). If the Court finds that it cannot distinguish and properly relegate *Miller*, it should overturn that ruling.

B. Congress Required a Warrant Because Disclosure of Communications Takes Something from an Unrepresented Party

This is not a "third-party subpoena" case, of course, though the government has pressed that framing. It involves a probable cause warrant. Congress called the process by that name and required the legal standard of a warrant to be met. 18 U.S.C. § 2703.

This is a warrant case because Congress recognized at least implicitly that the procedure it was creating would take something from customers of communica-

tions providers, and that the interests of those customers would not be fully defended by the communications providers. By contrast, the "third-party subpoena" acts as a warrant in terms of the personal and private information it discloses, but dispenses with the probable cause standard.

When probable cause exists, what the SCA allows to be taken from Microsoft customers is the right to exclude others from their communications and communications metadata. Customers of Microsoft have these property rights in their communications and data even though they typically do not generally possess the material that they store with that company.

To rationalize what has happened here, the Court should recognize that there is often a separation of possession from other property rights, such as the right to exclude, in the digital context. Careful legal characterization sets up the question before this Court: whether application of an SCA warrant requiring a company to retrieve its customer's data from overseas is "extraterritorial."

III. USING A WARRANT TO REQUIRE AN EMAIL-SERVICES PROVIDER TO RETRIEVE CUSTOMERS' DATA FROM OVERSEAS IS EXTRATERRITORIAL

Posit a federal statute that requires private parties to throw rocks on the instruction of the government. In most cases, commands to throw rocks will result in rocks being thrown and landing inside the United States. The directive, the action, and the result in such cases are purely domestic.

The statute might also be used to require a person facing north on the Canadian border to throw a rock.

The domestically given command for a domestic action would have an ineluctably extraterritorial result. Those are the predictable laws of physics at play.

Those same laws of physics are in operation when the requirement is not to throw rocks, but to copy or manipulate data. The typical SCA warrant is a domestic command for domestic activity with a domestic result. But when the object of the warrant is data housed overseas, the domestic command for a domestic action has an ineluctable extraterritorial result.

There is no serious argument undercutting the presumption against extraterritoriality as described in *Morrison v. National Australia Bank Ltd.*, 561 U.S. 247, 255 (2010), and *RJR Nabisco v. European Community*, 136 S. Ct. 2090, 2100 (2016). And there is no good argument that the SCA "affirmatively and unmistakably" provides for extraterritorial application. *Id*. Thus, the question is whether the "focus" of an SCA warrant is domestic.

At one level of abstraction, the warrant in this case has a purely domestic "focus." It was issued in service of domestic enforcement of narcotics trafficking laws, or at least enforcement of domestic U.S. laws. But analysis at that level overshoots all the justifications for the presumption against extraterritoriality. It would allow any command or regulation with extraterritorial effects to be excused by the idea that enforcement of a U.S. law may hang in the balance.

The better level of abstraction is the subject-matter level. The Stored Communications Act, as the name implies, deals with the protection and disclosure of stored communications. At both ends—protection and

disclosure—applying the SCA's focus to material housed overseas is extraterritorial and not domestic.

A. Applying the SCA as Privacy Legislation Here Would Be Extraterritorial

A major interest served by protection of stored communications is privacy. The term has varied meanings, but in the information context, privacy is rightly thought of as the condition one enjoys when exercising control of personal information consistent with one's interests and values. *See* Jim Harper, *Understanding Privacy—and the Real Threats to It*, Cato Institute, Policy Analysis No. 520 (2004). The Stored Communications Act's proscription on access to communications, *e.g.*, 18 U.S.C. § 2701, protects privacy.

Precisely where and when the Stored Communications Act protects privacy is somewhat metaphysical. It could be that the sense of control travels with the person, or it could be that the control is exercised where the data rests.[3]

Whatever the case, the better view is that the copying of data overseas to be delivered back to the United States is an essential step in undercutting control of information and thus privacy. In this case, the privacy

[3] At oral argument in the court below, the panel grilled respondent's counsel, Mr. Rosenkranz, on whether American law would apply if Microsoft sold data stored overseas to a tabloid. Somewhat provocatively, Mr. Rosenkranz insisted that American law would not apply. A finer statement of his case, if an American's data is involved, is that American *legislation* would not apply, but American consumers have contract and tort rights against Microsoft no matter where it stores data.

"focus" of the SCA points to an extraterritorial application or, at best, an ambiguous and changing application.

B. Application of the SCA as Disclosure Legislation Here Would Be Extraterritorial

The other arguable "focus" of the Stored Communications Act is disclosure. 18 U.S. Code § 2703. There is an argument that literal "disclosure" occurs only when the retrieved data is delivered to the government or even when government agents process it to reveal its content.

But that argument elides an essential step in disclosure of overseas material: retrieval of the information from the overseas location. Just as with privacy, if the SCA's "focus" is requiring and regulating disclosure, it is extraterritorial when applied to data held overseas.

Because of its extraterritorial application in this case, the SCA warrant is invalid. It is a warrant, though, not a subpoena or some other indefinite form of compelled disclosure. The reason why Congress correctly made it a warrant was the implicit recognition that the process takes something from the customer of a communications services provider. What it takes are certain property rights in the communications, which are originally allocated by contract. The Court should so find in affirming the court below, undaunted by certain narrow counterarguments.

IV. CONTRACT PRINCIPLES ANSWER POTENTIAL PROBLEMS

There are narrow arguments suggesting that property and contract law are not up to the task of framing the issues in this case. But proper application of contract principles rebuts those arguments.

A. Exceptions in Contracts for Legal Processes Assume and Require Validity

It can be argued that the contracts allocating property rights in data do not give Microsoft customers the right to restrict sharing of data with the government.

As noted above, both Microsoft policies include exceptions for sharing with law enforcement. "We may access or disclose information about you, including the content of your communications, in order to: . . . comply with the law or respond to lawful requests or legal process." 2013 Microsoft Contract. "[W]e will access, transfer, disclose, and preserve personal data . . . when we have a good faith belief that doing so is necessary to: … comply with applicable law or respond to valid legal process, including from law enforcement or other government agencies." Microsoft 2018 Contract.

Neither of these provisions gives Microsoft free rein to hand data over to the government when asked. Microsoft can only do so in response to "lawful requests or legal process" in the one case and "good faith belief that doing so is necessary to: . . . comply with applicable law or respond to valid legal process" in the other. Microsoft may not hand over information when the law does not require it, or when it is faced with something other than "lawful," "legal." and "valid" processes.

These words have two possible senses: (i) the procedures are recognized and systematically used in law enforcement and courts and (ii) the procedures comport with the standards laid out in the SCA and the Fourth Amendment.

In fair reading, neither contract version permits Microsoft to comply with court orders simply because they take a certain form. Such orders must also satisfy the substantive legal requirements for divesting a private party of control over the things demanded by the government. Microsoft only has the right to share the data if the process used to divest the customer of control is both legal in form and substance. To the extent Microsoft does not resist an invalid or overbroad warrant, the data is not Microsoft's to turn over. The data remains the property of the customer. Here, the otherwise-valid warrant is invalid because it is extraterritorial.

The argument that Microsoft must turn the data over because the warrant is a legal process begs the question whether the process is valid. In this case, the warrant requirement has been fulfilled, so the property right of the customer would be overcome, and the data would be turned over but for the extraterritorial application of the warrant.

B. Service Providers Are Unlikely to Place Data Offshore for Illegitimate Reasons

Another narrow challenge to the argument for recognition of contract-based property rights in data is that service providers may move data offshore for reasons congenial to criminals. Neither the criminal law nor contract law would allow this.

Were a company in Microsoft's position to place data offshore as part of a scheme to assist criminals, that practice would bring accessory and conspiracy criminal liability onto the company itself. There is no serious argument that recognizing the legitimate technical and business reasons for placing data offshore implies an open avenue to corporate participation in crime.

As a matter of contract law, agreements to hide data offshore would be void as contrary to public policy, a classic black-letter contracts concept. The criminal beneficiaries of any such arrangement could not enjoy the property rights purportedly created by it, and the information could be retrieved without violence to their non-existent property rights.

CONCLUSION

The extraterritoriality of the SCA when applied to overseas data is made clear by recognizing and carefully articulating the legal concepts at play. The warrant requirement set out by Congress is correctly framed as a warrant—it is not a subpoena or subpoena-like process—because something belonging to the Microsoft customer stands to be taken without according him or her an opportunity to object. That is precisely the circumstance that calls for review by a neutral magistrate—and that demands a warrant.

The thing that would be taken in such a seizure is not possession, but the right to exclude, which is "one of the most essential sticks in the bundle of rights that are commonly characterized as property." *Kaiser Aetna v. United States*, 444 U.S. 164, 176 (1979). In affirming and clarifying these legal principles, the Court should affirm the decision below.

Respectfully submitted,

Ilya Shapiro
Trevor Burrus
Reilly Stephens
CATO INSTITUTE
1000 Mass. Ave. N.W.
Washington, D.C. 20001
(202) 842-0200
ishapiro@cato.org

Jim Harper
Counsel of Record
COMPETITIVE ENTERPRISE INSTITUTE
1310 L St. NW, 7th Floor
Washington, D.C. 20005
(202) 331-1010
jim.harper@cei.org

Berin Szóka
TECHFREEDOM
110 Maryland Ave. N.E.
Suite 409
Washington, D.C. 20002
(202) 803-2867
bszoka@techfreedom.org

Manuel S. Klausner
LAW OFFICES OF MANUEL S. KLAUSNER
One Bunker Hill Building
601 W. Fifth St.,
Suite 800
Los Angeles, CA 90071
(213) 617-0414
mklausner@klausnerlaw.us

January 17, 2018