No. 20-1653(L)

No. 20-3945 (CON)

United States Court of Appeals

for the

Second Circuit

In re: In The Matter Of The Search of Information Associated with Specified E-Mail Accounts

MICROSOFT CORPORATION,

Appellant,

– v. –

UNITED STATES OF AMERICA,

Appellee.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF NEW YORK

BRIEF FOR *AMICI CURIAE* THE CHAMBER OF COMMERCE OF THE UNITED STATES OF AMERICA, CENTER FOR DEMOCRACY AND TECHNOLOGY, INTERNET ASSOCIATION, AND NATIONAL ASSOCIATION OF MANUFACTURERS IN SUPPORT OF APPELLANT

Andrew J. Pincus
Counsel of Record
MAYER BROWN LLP
1999 K Street, NW
Washington, DC 20006
(202) 263-3000
apincus@mayerbrown.com

Counsel for Amici Curiae

(Continued on inside cover)

Tara S. Morrissey
U.S. CHAMBER LITIGATION CENTER, INC.
1615 H Street, NW
Washington, DC 20062
(202) 463-5337

Counsel for the Chamber of Commerce of the United States of America

CORPORATE DISCLOSURE STATEMENT

None of the *amici curiae* has a parent corporation. No publicly held corporation owns 10 percent or more of the stock of any of the *amici*.

TABLE OF CONTENTS

Page

STATEMENT OF INTEREST 1

INTRODUCTION AND SUMMARY OF ARGUMENT 3

ARGUMENT 6

I. THE SCA'S AUTHORIZATION OF SURREPTITIOUS SEARCHES OF DATA HOSTED IN THE CLOUD THREATENS SIGNIFICANT ADVERSE CONSEQUENCES FOR U.S. INDIVIDUALS AND BUSINESSES. 6

A. Cloud computing offers very substantial advantages over local storage 7

B. Weakened protections against unjustified government surveillance will undermine user trust, discourage the adoption of cloud computing, and disadvantage American companies. 11

II. COURTS MUST EVALUATE APPLICATIONS FOR SECRECY ORDERS UNDER THE STRICT SCRUTINY STANDARD. 13

A. SCA gag orders are subject to strict scrutiny because they are content-based prior restraints on a cloud services provider's speech. 14

B. Strict scrutiny is also warranted because gag orders effectively vitiate the rights of provider's customers. 16

1. Orders requiring service providers to turn over customer data under § 2703 are "searches" under the Fourth Amendment. 17

2. Notice of government searches is critical to enable data owners to vindicate Fourth Amendment and other rights. 19

III. THE DISTRICT COURT FAILED TO APPLY THE REQUIRED STRICT SCRUTINY TO THE APPLICATION IN THIS CASE. 22

CONCLUSION 27

TABLE OF AUTHORITIES

Page(s)

Cases

Abourezk v. Reagan,
785 F.2d 1043 (D.C. Cir. 1986).....26

Bantam Books, Inc. v. Sullivan,
372 U.S. 58 (1963).....15

Camara v. Municipal Court of City and Cty. of S.F.,
387 U.S. 523 (1967).....17

Carpenter v. United States,
138 S. Ct. 2206 (2018).....18, 19, 22

Citizens United v. FEC,
558 U.S. 310 (2010).....17

City of Boerne v. Flores,
521 U.S. 507 (1997).....14

Dalia v. United States,
441 U.S. 238 (1979).....21

FW/PBS, Inc. v. City of Dallas,
493 U.S. 215 (1990).....15

John Doe, Inc. v. Mukasey,
549 F.3d 861 (2d Cir. 2008) 14

Kyllo v. United States,
533 U.S. 27 .....18, 22

Microsoft Corp. v. U.S. Dep't of Justice,
233 F. Supp. 3d 887 (W.D. Wash. 2017) 20

In re National Sec. Letter,
863 F.3d 1110 (9th Cir. 2017) 16

TABLE OF AUTHORITIES
(continued)

Page(s)

Nebraska Press Ass'n v. Stuart,
427 U.S. 539 (1976).....15, 23

Olmstead v. United States,
277 U.S. 438 (1928).....7

Reed v. Town of Gilbert,
576 U.S. 155 (2015).....15

Reno v. American Civil Liberties Union,
521 U.S. 844 (1997).....24

Riley v. California,
573 U.S. 373 (2014).....6, 11, 18, 22

In re Sealing and Non-Disclosure of Pen/Trap/2703(d),
562 F. Supp. 2d 876 (S.D. Tex. 2008).....15

Sorrell v. IMS Health Inc.,
564 U.S. 552 (2011).....14

Matter of Subpoena 2018R00776,
947 F.3d 148 (3d Cir. 2020) 16, 25

United States v. Martinez,
498 F.2d 464 (6th Cir. 1974) 21

United States v. Playboy Entm't Grp., Inc.,
529 U.S. 803 (2000).....5, 15

United States v. Salameh,
992 F.2d 445 (2d Cir. 1993) 23

United States v. Villegas,
899 F.2d 1324 (2d Cir. 1990) 22

United States v. Warshak,
631 F.3d 266 (6th Cir. 2010) 17, 18

TABLE OF AUTHORITIES
(continued)

Page(s)

In the Matter of Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., 829 F.3d 197 (2d Cir. 2016) 17

Statutes and Rules

18 U.S.C. § 2518(8)(d).....21

18 U.S.C. § 2703(b) 4, 20

18 U.S.C. § 2703(d) 18

18 U.S.C. § 2705(a) 15

18 U.S.C. § 2705(b) .....*passim*

Other Authorities

Damon C. Andrews & John M. Newman, *Personal Jurisdiction and Choice of Law in the Cloud*, 73 Md. L. Rev. 313 (2013).....9

Lee Badger et al., Recommendations of the Nat'l Inst. of Standards & Tech., U.S. Dep't of Commerce, *NIST Special Publication 800-146: Cloud Computing Synopsis and Recommendations*, at Sec. 5.3.3-5.4 (2012), https://bit.ly/37uuzrD.....9

Berkman Center for Internet & Society at Harvard University, *Don't Panic: Making Progress on the "Going Dark" Debate* (2016), https://bit.ly/3amuJD6.....12

Nicholas Bloom & Nicola Pierri, *Cloud Computing Is Helping Smaller, Newer Firms Compete*, Harv. Bus. Rev. (Aug. 31, 2018), https://bit.ly/3gXD4Pa 9

Sara Castellanos, *Covid-19 Pandemic Underscored Importance of IT in Medical Research*, Wall St. J. (Nov. 13, 2020), https://on.wsj.com/2Wk0KUo 11

TABLE OF AUTHORITIES
(continued)

Page(s)

Daniel Castro & Alan McQuinn, *Beyond the USA Freedom Act: How U.S. Surveillance Still Subverts U.S. Competitiveness* (June 2015), https://bit.ly/3r05xs3 12

Elizabeth Dwoskin & Frances Robinson, *NSA Internet Spying Sparks Race to Create Offshore Havens for Data Privacy*, Wall St. J. (Sept. 27, 2013), https://on.wsj.com/2K4yL8L 12

Arul Elumalai et al., *Making A Secure Transition to the Public Cloud*, *in* McKinsey Digital, *Creating Value with the Cloud* at 27 (Dec. 2018), https://mck.co/37m4fQn 8

Jared A. Harshbarger, *Cloud Computing Providers and Data Security Law: Building Trust with United States Companies*, 16 J. Tech. L. & Pol'y 229 (2011) 9

Christopher Hooton, *Examining the Economic Contributions of the Cloud to the United States* (Mar. 5, 2019) 8

Nancy J. King & V.T. Raja, *What Do They Really Know About Me in the Cloud? A Comparative Law Perspective on Protecting Privacy and Security of Sensitive Consumer Data*, 50 Am. Bus. L.J. 413, 418 (2013) 7

Gartner, *Gartner Forecasts Worldwide Public Cloud Revenue to Grow 6.3% in 2020* (July 23, 2020), https://gtnr.it/37iZ7fM 8

McKinsey Digital, *Creating Value with the Cloud* (Dec. 2018), https://mck.co/37m4fQn 8

Aaron Tilley, *One Business Winner Amid the Coronavirus Lockdowns: the Cloud*, Wall St. J. (Mar. 27, 2020), https://on.wsj.com/3h42Otg 10

Kevin Werbach, *The Network Utility*, 60 Duke L.J. 1761 (2011) 8

Alex Woodie, *Storage in the Exabyte Era*, Datanami (Feb. 19, 2020), https://bit.ly/3oYa9NF 11

TABLE OF AUTHORITIES
(continued)

Page(s)

U.S. Dep't of Justice, *Policy Regarding Applications for Protective Orders Pursuant to 18 U.S.C. § 2705(b)*, at 2 (Oct. 19, 2017), https://www.justice.gov/criminal-ccips/page/file/1005791/download 15

STATEMENT OF INTEREST[1]

The Chamber of Commerce of the United States of America is the world's largest business federation. The Chamber represents approximately 300,000 direct members and indirectly represents the interests of more than three million companies and professional organizations of every size, in every industry sector, and from every region of the country. An important function of the Chamber is to represent the interests of its members in matters before Congress, the Executive Branch, and the courts. To that end, the Chamber regularly files *amicus curiae* briefs in cases that raise issues of concern to the nation's business community.

The Center for Democracy & Technology ("CDT") is a nonprofit public interest group that seeks to put democracy and individual rights at the center of the digital revolution. CDT supports laws, corporate policies, and technical tools that protect the civil liberties of internet users and represents the public's interest in maintaining an open internet. In furtherance of this mission, CDT supports legal and policy decisions that preserve individual rights, are based on a thorough understanding of how technologies work, and promote the overall security of the

---

[1] No counsel for a party authored this brief in whole or in part, and no person other than the *amici curiae*, their members, or their counsel contributed money that was intended to fund the preparation or submission of this brief. *See* Fed. R. App. P. 29(a)(4)(E). All parties consented to the filing of this brief. *See* Fed. R. App. P. 29(a)(2).

internet and its users. CDT frequently files *amicus* briefs in cases involving constitutional protections for users of online technologies.

Internet Association ("IA") is the only trade association that exclusively represents leading global internet companies on matters of public policy. IA's mission is to foster innovation, promote economic growth, and empower people through the free and open internet. A list of IA's members is available at https://internetassociation.org/our-members/.

The National Association of Manufacturers (NAM) is the largest manufacturing association in the United States, representing small and large manufacturers in every industrial sector and in all 50 states. Manufacturing employs more than 12 million men and women, contributes roughly $2.05 trillion to the U.S. economy annually, has the largest economic impact of any major sector, and accounts for nearly two-thirds of private-sector research and development in the Nation. The NAM is the voice of the manufacturing community and the leading advocate for a policy agenda that helps manufacturers compete in the global economy and create jobs across the United States. The Manufacturers' Center for Legal Action—the litigation arm of the NAM—advocates on behalf of the manufacturers in the courts.

Amici represent users and providers of cloud computing, which as explained below provides substantial benefits to individuals, businesses, and the entire U.S.

economy. Those benefits are jeopardized, and the rights of cloud computing users threatened, when district courts too readily defer to the government's demand for secrecy as it searches data stored in the cloud in connection with law enforcement investigations. Accordingly, each *amici* has a keen interest in ensuring that the laws pertaining to government surveillance of electronic data are enforced in conformance with the Constitution's requirements.

INTRODUCTION AND SUMMARY OF ARGUMENT

Before the technological advances of the last several decades, individuals and businesses kept important, private information on their own premises, either in physical form or stored in their own computer systems. If the government wanted access to that information, it usually had to serve a warrant on the individual or business —and the individual or business could contest the government's demand or argue that some or all of the information sought was protected against disclosure by privileges, such as the attorney-client or work-product privilege.

Today, however, "cloud computing" providers such as Google, Microsoft, and Amazon offer individuals and businesses the ability to host all of their commercial and personal information—business plans, legal advice, emails, photos, and other sensitive data—on remote servers. These services provide significant benefits by reducing costs, improving efficiency, and spurring innovation.

But—because the confidential information of individuals and businesses is held by a third party (the cloud services provider)—the government can, and does, leverage this new technology to obtain increasing amounts of confidential data without the knowledge of the data's owner.

The government routinely invokes its authority under Title II of the Electronic Communications Privacy Act (the Stored Communications Act or "SCA") to force third-party service providers to turn over customer data stored "in the cloud." The SCA does not require the government to give the customer prior notice that the government is seeking to force a third-party service provider to disclose the customer's data in connection with a law enforcement investigation. 18 U.S.C. § 2703(b). And the SCA authorizes—and the government frequently obtains—*ex parte* gag orders forbidding the third-party provider from notifying its customers of the government's demand. 18 U.S.C. § 2705(b).

These gag orders greatly enhance the government's power because—in sharp contrast to the regime prevailing before the advent of cloud computing—the owner of the information has no idea that the government seeks to obtain confidential information, and therefore does not have any opportunity to invoke limits on the government's authority or to assert privileges that protect against disclosure of some or all of the information sought by the government.

The gag orders issued under the SCA are content-based prior restraints that effectively eliminate the ability of a company or individual to assert Fourth Amendment rights or applicable privileges—and therefore are permissible only if the government satisfies the strict scrutiny standard. A gag order accordingly must be justified by facts showing that the order is narrowly tailored to promote a compelling state interest, and that there is no less restrictive alternative that furthers those aims. *United States v. Playboy Entm't Grp., Inc.*, 529 U.S. 803, 813 (2000). Here, although the district court articulated the correct test, it misapplied that standard by deferring to the government without rigorous consideration of the alternatives available to protect the government's asserted interests.

Erroneously-issued gag orders violate the free-speech rights of the third-party provider and, in addition, vitiate the ability of the provider's customers—both individuals and businesses—to assert their own legal rights, putting American cloud service providers at a marked disadvantage in the marketplace, and undermining users' trust in cloud services. This Court should reaffirm the applicability of the strict scrutiny standard and require district courts to assess the government's gag order requests under the rigorous requirements that apply to similar content-based prior restraints on First Amendment rights.

ARGUMENT

I. THE SCA'S AUTHORIZATION OF SURREPTITIOUS SEARCHES OF DATA HOSTED IN THE CLOUD THREATENS SIGNIFICANT ADVERSE CONSEQUENCES FOR U.S. INDIVIDUALS AND BUSINESSES.

"Cloud computing is the capacity of Internet-connected devices to display data stored on remote servers rather than on the device itself." *Riley v. California*, 573 U.S. 373, 397 (2014). Cloud technology has revolutionized many aspects of modern life, making new products and services available, transforming the way people work and interact, and allowing businesses to be more efficient, nimble, and productive. But that technology also raises very significant questions regarding protections against unjustified government surveillance.

Historically, individuals and businesses kept most sensitive information and documents on their premises, behind locked doors or in filing cabinets. Later, individuals and businesses stored information electronically on private servers or backup drives that were not accessible to third parties. If the government sought access to those materials, it had to serve a warrant—and the owner of the information could contest the legitimacy of the warrant in court, assert applicable privileges, or take other steps to protect their legal interests.

The move to the cloud means that vast amounts of confidential information now reside in third-party servers located hundreds or thousands of miles away from the information's owner. Federal law permits the government to obtain that

information by serving process on the third party, and authorizes the government to seek a gag order barring the third party from informing the data owner of the government's demand. *Cf. Olmstead v. United States*, 277 U.S. 438, 473-74 (1928) (Brandeis, J., dissenting) ("Ways may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home.").

Cloud technology was built to increase efficiency, scalability, and cybersecurity—not to undermine the ability of the owners of information to control that information and maintain its confidentiality. If moving information from a desktop computer or private server to the cloud results in reduced legal protection from government demands, then individuals and businesses naturally will be more reluctant to use this new technology. These consequences make it critically important that courts strictly enforce legal limitations on the government's ability to obtain data held in the cloud without the knowledge of the information's owner.

A. Cloud computing offers very substantial advantages over local storage.

Cloud computing has been called "one of the most significant technical advances for global business in this decade—as important as PCs were to the 1970s." Nancy J. King & V.T. Raja, *What Do They Really Know About Me in the Cloud? A Comparative Law Perspective on Protecting Privacy and Security of Sensitive*

Consumer Data, 50 Am. Bus. L.J. 413, 418 (2013). In 2018, eighty percent of companies surveyed reported that they expected to make significant use of public-cloud platforms in the near future. Arul Elumalai et al., *Making A Secure Transition to the Public Cloud*, *in* McKinsey Digital, *Creating Value with the Cloud* at 27 (Dec. 2018), https://mck.co/37m4fQn. One study estimates that cloud services resulted in over 2.15 million jobs and more than $210 billion of additional U.S. GDP in 2017 alone. Christopher Hooton, *Examining the Economic Contributions of the Cloud to the United States* (Mar. 5, 2019), Internet Ass'n, at 6, https://bit.ly/3qZqeEv. Worldwide revenues, currently forecast at $257 billion, are projected to rise to $364 billion in 2022. Gartner, *Gartner Forecasts Worldwide Public Cloud Revenue to Grow 6.3% in 2020* (July 23, 2020), https://gtnr.it/37iZ7fM.

Cloud computing technology offers numerous advantages to businesses and their customers.

First, the ability to access data from a remote data center creates significant economies of scale, resulting in reduced costs and better performance. A cloud computing provider can provide data backup services and business continuity, security, and other data operation functions far more efficiently—and reliably—than individual businesses. Kevin Werbach, *The Network Utility*, 60 Duke L.J. 1761, 1821-22 (2011).

In addition, because "companies share virtual capacity in massive clouds," large remote data centers provide a more efficient solution to fluctuating demand. *Id*. at 1822. Cloud service providers offer a pool of servers to customers who can rapidly harness those servers' collective computing power when needed ("scaling up") and rapidly release that power when the task is complete ("scaling down"). Damon C. Andrews & John M. Newman, *Personal Jurisdiction and Choice of Law in the Cloud*, 73 Md. L. Rev. 313, 325 (2013). Cloud computing has been especially important for small start-ups that cannot afford to build and maintain large data centers of their own. As one pair of commentators put it, the cloud has "democratized computing" and thereby increased competition and innovation across a variety of industries. Nicholas Bloom & Nicola Pierri, *Cloud Computing Is Helping Smaller, Newer Firms Compete*, Harv. Bus. Rev. (Aug. 31, 2018), https://bit.ly/3gXD4Pa.

Second, cloud computing providers' scale enables them to apply greater resources and expertise to protect against hacks and other unlawful intrusions than a business, university, government, or individual managing its own computer systems in-house. Jared A. Harshbarger, *Cloud Computing Providers and Data Security Law: Building Trust with United States Companies*, 16 J. Tech. L. & Pol'y 229, 234 (2011). Internet-based computing similarly provides businesses with disaster recovery services on a much more cost-efficient basis. Lee Badger et al., Recommendations of the Nat'l Inst. of Standards & Tech., U.S. Dep't of Commerce,

NIST Special Publication 800-146: Cloud Computing Synopsis and Recommendations, at Sec. 5.3.3-5.4 (2012), https://bit.ly/37uuzrD.

Third, cloud computing makes data more accessible for those who have permission to use it. Because a user can access and manipulate data from any location in the world that has an Internet connection, cloud computing makes it possible for a user to seamlessly create a document on a home laptop, edit it on a tablet, review it on a desktop computer at work, and then share it with colleagues around the globe.

The public health emergency that has unfolded over the last ten months provides a dramatic illustration of cloud computing's benefits. Virtually overnight, many jurisdictions declared stay-at-home orders due to coronavirus, many American workers stopped going into the office and canceled business travel, and individuals and companies vastly increased their use of videoconferencing, file-sharing, and other remote and cloud-based technologies. Demand for cloud services surged as a result. Aaron Tilley, *One Business Winner Amid the Coronavirus Lockdowns: the Cloud*, Wall St. J. (Mar. 27, 2020), https://on.wsj.com/3h42Otg.

This shift would not have been conceivable even a decade ago, when remote computing infrastructure was not yet widely available. Cloud computing not only made it possible for millions of Americans to work and collaborate from home during COVID-19; it played a critical role in processing and analyzing the vast

amounts of data scientists needed to understand and treat the virus. Sara Castellanos, *Covid-19 Pandemic Underscored Importance of IT in Medical Research*, Wall St. J. (Nov. 13, 2020), https://on.wsj.com/2Wk0KUo.

B. Weakened protections against unjustified government surveillance will undermine user trust, discourage the adoption of cloud computing, and disadvantage American companies.

Although cloud computing has lowered costs, created efficiencies, and unleashed new products and services, it has also raised important and novel privacy concerns.

To begin with, the amount of information involved is staggering—and growing every year. The Supreme Court recently observed that a single smartphone can store a gigantic array of information:

> The current top-selling smart phone has a standard capacity of 16 gigabytes (and is available with up to 64 gigabytes). Sixteen gigabytes translates to millions of pages of text, thousands of pictures, or hundreds of videos. . . . The storage capacity of cell phones has several interrelated consequences for privacy.

Riley, 573 U.S. at 394. The cloud computers that support smartphones and a myriad of other devices store amounts of information that make smartphones trivial in comparison. Experts expect that many enterprise clients will soon need to measure their storage requirements in exabytes—*billions* of gigabytes—or more. *See* Alex Woodie, *Storage in the Exabyte Era*, Datanami (Feb. 19, 2020), https://bit.ly/3oYa9NF.

The growing size and scope of data stored in the cloud has led to a corresponding increase in government demands for access to that information from cloud services providers, and providers have responded to concerns about unjustified government surveillance by providing tools and other mechanisms to ensure greater data security. *See, e.g.*, Berkman Center for Internet & Society at Harvard University, *Don't Panic: Making Progress on the "Going Dark" Debate*, at 3-4 (2016), https://bit.ly/3amuJD6. However, the perception that cloud providers cannot keep data safe from law enforcement or government officials remains significant for all U.S. service providers—regardless of which providers receive data requests from the U.S. government in a particular period.

After the public disclosure of the National Security Agency's PRISM program in 2013, for example, many entities canceled contracts with American companies. One report found that the damage due to public perceptions about U.S. government surveillance would "likely far exceed" $35 billion. Daniel Castro & Alan McQuinn, *Beyond the USA Freedom Act: How U.S. Surveillance Still Subverts U.S. Competitiveness* (June 2015), https://bit.ly/3r05xs3; *see also* Elizabeth Dwoskin & Frances Robinson, *NSA Internet Spying Sparks Race to Create Offshore Havens for Data Privacy*, Wall St. J. (Sept. 27, 2013), https://on.wsj.com/2K4yL8L (explaining that foreign countries "are seeking to use data-privacy laws as a competitive advantage—a way to boost domestic companies that long have sought an edge over

Google, Microsoft Corp. and other U.S. tech giants"). Concerns about potential government access to data hosted by third parties remain a key consideration for individuals and businesses using cloud services and threaten the competitiveness of U.S. companies in the global economy.

II. COURTS MUST EVALUATE APPLICATIONS FOR SECRECY ORDERS UNDER THE STRICT SCRUTINY STANDARD.

One way that cloud services providers reassure customers regarding the security of their information is by promising that—to the extent permitted by law—they will inform the affected customer of government requests for a customer's data, so that the customer will be able to assert the same protections against disclosure that could have been invoked when the data was stored on the customer's own servers. SCA gag orders impose a prior restraint on providers' speech regarding an issue of great interest to providers' customers—both those who learn of government access to their information and those whose information is not sought but who learn of the extent to which the government searches or seizes information held by their provider for other customers. The speech restrained by these orders also relates to a topic of general public interest: government surveillance of electronic data. The orders therefore must satisfy strict scrutiny to pass constitutional muster.

A. SCA gag orders are subject to strict scrutiny because they are content-based prior restraints on a cloud services provider's speech.

A gag order under the SCA precludes third-party providers from "notify[ing] any other person of the existence of the warrant, subpoena, or court order." 18 U.S.C. § 2705(b). It is therefore a content-based restriction that restrains providers from speaking publicly about a particular subject matter—the SCA warrant, subpoena, or court order in question—for as long as the order is in effect. *Sorrell v. IMS Health Inc.*, 564 U.S. 552, 564 (2011).

The SCA requires an applicant for a gag order to show that there is "reason to believe" that notification of the warrant, subpoena, or court order will result in one or more adverse consequences. 18 U.S.C. § 2705(b). This Court has interpreted materially similar language in the National Security Letter context, 18 U.S.C. § 3511(b)(2), to require "*good* reason to believe" that the gag order is necessary. *John Doe, Inc. v. Mukasey*, 549 F.3d 861, 875-76 (2d Cir. 2008) (emphasis added). However, even this enhanced reading falls short of constitutional requirements.

That is because content-based restrictions cannot be imposed merely because there is "good reason" to believe that speech will lead to adverse results. Rather, such restrictions are subject to strict scrutiny—the "most demanding test known to constitutional law." *City of Boerne v. Flores*, 521 U.S. 507, 534 (1997). Under that standard, content-based restrictions "are presumptively unconstitutional and may be

justified only if the government proves that they are narrowly tailored to serve compelling state interests." *Reed v. Town of Gilbert*, 576 U.S. 155, 163 (2015); *see also Playboy*, 529 U.S. at 813.

A gag order is also subject to strict scrutiny because it is a prior restraint—one of "the most serious and least tolerable infringement on First Amendment rights." *Nebraska Press Ass'n v. Stuart*, 427 U.S. 539, 559 (1976). "Any system of prior restraints of expression comes . . . bearing a heavy presumption against its constitutional validity." *Bantam Books, Inc. v. Sullivan*, 372 U.S. 58, 70 (1963). And prior restraints that last indefinitely are especially suspect. *See In re Sealing and Non-Disclosure of Pen/Trap/2703(d)*, 562 F. Supp. 2d 876, 886 (S.D. Tex. 2008) ("An indefinite nondisclosure order is tantamount to a permanent injunction of prior restraint."); *cf. FW/PBS, Inc. v. City of Dallas*, 493 U.S. 215, 226 (1990) ("a prior restraint that fails to place limits on the time within which the decisionmaker must issue the license [to speak] is impermissible"). The SCA does not limit gag orders to any particular duration.[2]

[2] *Compare* 18 U.S.C. § 2705(a) (authorizing an order providing for delayed notice to the target of the subpoena or order "for a period not to exceed ninety days") *with id.* § 2705(b) (authorizing a gag order "for such period as the court deems appropriate"). In 2017, the Department of Justice issued guidance stating that "[b]arring exceptional circumstances, prosecutors filing § 2705(b) applications may only seek to delay notice for one year or less." U.S. Dep't of Justice, *Policy Regarding Applications for Protective Orders Pursuant to 18 U.S.C. § 2705(b)*, at 2 (Oct. 19, 2017), https://www.justice.gov/criminal-ccips/page/file/1005791/download. However, the Department's policy is intended "only to improve the

Both the Third Circuit and the Ninth Circuit have for these reasons concluded that the strict scrutiny standard applies to gag orders precluding providers from engaging in speech regarding requests for their customer's data. The Third Circuit held that Section 2705(b) orders are subject to strict scrutiny as content-based restrictions that prohibit the recipient "from conveying information about a grand jury investigation, thus draw[ing] distinctions based on the message"; and as prior restraints, "forbidding certain communications . . . in advance of the time that such communications are to occur.'" *Matter of Subpoena 2018R00776*, 947 F.3d 148, 155 (3d Cir. 2020) (internal quotations omitted).

The Ninth Circuit held that a similar gag order under the National Security Letter statute triggered strict scrutiny because it was a content-based restriction that "prohibits speech about one specific issue: the recipient may not 'disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records'" through a national security letter. *In re National Sec. Letter*, 863 F.3d 1110, 1123 (9th Cir. 2017).

B. Strict scrutiny is also warranted because gag orders effectively vitiate the rights of provider's customers.

Applying strict scrutiny to gag orders under § 2705(b) is also appropriate because those orders preclude the owner of the information from asserting his or her

---

internal management of the Department of Justice," and the Department expressly contemplates that orders of a longer duration may be necessary. *Id*. at 1 n.1 & 2 n.3.

Fourth Amendment rights and, in addition, privileges that protect against disclosure of information to the government. *See United States v. Warshak*, 631 F.3d 266, 283, 292 (6th Cir. 2010) (challenging government's access to presumptively privileged emails pursuant to a search warrant and SCA order). Like the Fourth Amendment—the "basic purpose" of which is "to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials," *Camara v. Municipal Court of City and Cty. of S.F.*, 387 U.S. 523, 528 (1967)—the First Amendment is "[p]remised on mistrust of governmental power." *Citizens United v. FEC*, 558 U.S. 310, 340 (2010). It therefore makes sense to apply the strict scrutiny standard to government restrictions on speech necessary to protect Fourth Amendment rights.

1. *Orders requiring service providers to turn over customer data under § 2703 are "searches" under the Fourth Amendment.*

This Court has recognized that the government's ability to use the SCA to obtain a customer's data from its third-party provider, rather than directly from the customer's computer systems, does not make the SCA order any less of a search under the Fourth Amendment. *In the Matter of Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp.*, 829 F.3d 197, 214 (2d Cir. 2016) ("[w]hen the government compels a private party to assist it in conducting a search or seizure, the private party becomes an agent of the government" and the Fourth Amendment's warrant clause applies), *vacated as moot by United States v. Microsoft Corp.*, 138 S. Ct. 1186 (2018). Just as "the police may not storm the post

office and intercept a letter . . . unless they get a warrant," so, too, must they obtain a warrant to search a user's e-mail account hosted by a third-party service provider. *Warshak*, 631 F.3d at 286 (holding that e-mails in the possession of third parties are protected by the Fourth Amendment).

To hold otherwise would allow the government to use new technology—the remote storage of data in the cloud—to radically transform the expectations of privacy that individuals and businesses enjoy in their personal data. As the Supreme Court has repeatedly held, however, the Fourth Amendment does not leave individuals "at the mercy of advancing technology." *Kyllo v. United States*, 533 U.S. 27, 34-35(2001); *see also Riley*, 573 U.S. at 397-98.

Carpenter v. United States, 138 S. Ct. 2206 (2018), confirms that when information would be protected by the Fourth Amendment if stored on the user's premises in physical form or on a user's laptop or smart phone, the information does not lose that protection merely because the information is stored with a third party in the cloud. In *Carpenter*, the Supreme Court held that the Fourth Amendment's protections applied to the use of 18 U.S.C. § 2703(d) to obtain cell-site location information from a suspect's cell phone provider in order to track the target's physical movements. The Court recognized that this tracking information, like cloud data, "is detailed, encyclopedic, and effortlessly compiled," and "[w]ith just the click of a button, the Government can access each carrier's deep depository of historical

location information at practically no expense." 138 S. Ct. 2216-18. Thus, the Court concluded, "the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection." *Id*.

As the Court further explained, "[c]ell phone location information is not truly 'shared' as one normally understands the term," for carrying one is "indispensable to participation in modern society," and "a cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up." *Carpenter*, 138 S. Ct. at 2220. The same reasoning applies to the data that individuals and businesses store in the cloud in order to participate in many activities of modern life. *See supra* Part IA.

2. *Notice of government searches is critical to enable data owners to vindicate Fourth Amendment and other rights.*

The Fourth Amendment's protections against unjustified government intrusions provide little benefit when the owner of the information cannot assert those protections—because he is unaware that the government is seeking his information. The same is true of other rights belonging to the data owner, such as the attorney-client privilege and other similar protections.

Notice is crucial in the context of the SCA because providers who receive a warrant for hosted data are unlikely to seek to assert Fourth Amendment claims themselves. Indeed, some courts have held that remote computing providers simply lack standing to bring Fourth Amendment claims on behalf of their customers. *E.g.*,

Microsoft Corp. v. U.S. Dep't of Justice, 233 F. Supp. 3d 887, 916 (W.D. Wash. 2017) ("The court acknowledges the difficult situation this doctrine creates for customers subject to government searches and seizures under Sections 2703 and 2705(b)."). And providers will not know whether the information sought by the government includes legal advice or other privileged communications; neither will providers have an incentive to litigate those issues.

The SCA, however, specifically relieves the government of the obligation to provide notice to a customer when (as here) a search is conducted pursuant to a warrant, 18 U.S.C. § 2703(b)(1)(A), and then permits the government to bar the cloud services provider—the only other entity capable of informing the customer of the government's demand—from giving notice as well. *Id*. § 2705(b).

"The combined effect of §§ 2703(b)(1)(A) and 2705(b)," courts have recognized, "is that the subscriber may never receive notice of a warrant to obtain content information from a remote computing service and the government may seek an order under § 2705(b) that restrains the provider indefinitely from notifying the subscriber." *In re Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2705(b)*, 131 F. Supp. 3d 1266, 1271-72 (D. Utah 2015). As a result, "some . . . customers will be practically unable to vindicate their own Fourth Amendment rights." *Microsoft*, 233 F. Supp. 3d at 916.

Indeed, the SCA's allowance for indefinite gag orders itself may give rise to a Fourth Amendment violation. In *Wilson v. Arkansas*, the Supreme Court addressed "whether the common-law knock and announce principle forms a part of the Fourth Amendment reasonableness inquiry." 514 U.S. 927, 930 (1995). After finding that this notice principle existed in England under the common law and "was woven quickly into the fabric of early American law," *id*. at 933, the Court concluded that notice was an essential part of the reasonableness analysis. *Id*. at 936. This was true even though certain limited circumstances—such as a threat of physical violence—may justify an unannounced entry. *See id*. at 935-36.[3]

Similarly, in *United States v. Freitas*, the Ninth Circuit, discussing a warrant that authorized surreptitious entry to a home, stated that "the absence of any notice requirement in the warrant casts strong doubt on its constitutional adequacy." 800 F.2d 1451, 1456 (9th Cir. 1986). That is "because surreptitious searches and seizures strike at the very heart of the interests protected by the Fourth Amendment," and

[3] To be sure, the Fourth Amendment does not always require advance notice of a search. For example, the Supreme Court has held that the Wiretap Act provides a "constitutionally adequate substitute for advance notice" by providing that "once the surveillance operation is completed the authorizing judge must cause notice to be served on those subjected to surveillance." *Dalia v. United States*, 441 U.S. 238, 248 (1979); *see also United States v. Martinez*, 498 F.2d 464, 468 (6th Cir. 1974) ("We believe that the provisions of 18 U.S.C. § 2518(8)(d) which direct that an inventory be served upon the persons named in the order and others affected by it satisfy the Fourth Amendment requirement of notice."). But the SCA's warrant provisions—which provide for *no* notice to the target and a potentially unlimited gag order on the provider—do not satisfy that standard.

therefore notice should be given within a short period of the incursion "except upon a *strong* showing of *necessity*." *Id*. (emphasis added); *see also United States v. Villegas*, 899 F.2d 1324, 1336-37 (2d Cir. 1990) ("if a delay in notice is to be allowed, the court should nonetheless require the officers to give the appropriate person notice of the search within a reasonable time after the covert entry").

In short, requiring the government to satisfy strict scrutiny in order to preclude a provider from giving notice to its customer not only protects the provider's rights under the First Amendment, but also the customer's rights under the Fourth Amendment. If the information sought by the government under the SCA were in physical form inside an individual's home or a business's office, notice to the data owner generally would be necessary, and the owner could take steps to assert applicable rights or privileges. Routinely dispensing with that notice when the data is obtained from the cloud allows the government to leverage a new technology to significantly reduce privacy protections—the precise outcome that the Supreme Court refused to permit in *Carpenter*, *Riley*, and *Kyllo*.

III. THE DISTRICT COURT FAILED TO APPLY THE REQUIRED STRICT SCRUTINY TO THE APPLICATION IN THIS CASE.

Although the district court concluded that strict scrutiny was the "appropriate standard of review" under the First Amendment (JA-90), it failed to apply that standard properly. The district court's substantive analysis of the original gag order

(JA 92-94)—and its assessment of the order's subsequent extension (JA-109-110)—were critically flawed in several ways.

First, the district court relied on the "risk" that other employees, "including higher-ups" at the company, were involved in the conspiracy. JA-93. But that risk will virtually always be present when the government seeks to obtain data from a business customer. For example, the district court stated that the "targeted employees did not attempt to conceal their conduct" and "used their company email addresses"—something that will be true any time government investigators seek to obtain copies of company emails. *Id*.

A mere "risk" cannot satisfy strict scrutiny, especially when, as here, the provider has suggested a variety of ways to reduce that risk and the district court failed to adequately explain why those approaches were insufficient. *See Nebraska Press Ass'n*, 427 U.S. at 568-70 ("risk that pretrial news accounts" could have "some adverse impact" on potential jurors did not establish "the requisite degree of certainty to justify restraint"); *United States v. Salameh*, 992 F.2d 445, 447 (2d Cir. 1993) (order prohibiting attorney statements that "*may* have something to do with the case" was unconstitutional where "[t]he record does not support a conclusion that no reasonable alternatives to a blanket prohibition exist") (emphasis in original).

Second, the district court required Microsoft to show that its less restrictive alternative was "as effective" as a gag order in maintaining the secrecy of the

government's criminal investigation. JA-93-94. That stacked the deck against Microsoft, because by definition keeping silent about the existence of a warrant will *always* protect secrecy more than disclosure, even if that disclosure is limited and sufficient to protect the government's interests. The case the district court relied on, *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997), struck down a restriction on Internet speech after finding no evidence of findings or hearings addressing potentially less restrictive alternatives to the challenged statutory scheme. *Reno* thus demonstrates that there is a "heavy burden on the *Government* to explain why a less restrictive provision would not be as effective" to satisfy strict scrutiny, even if those alternatives are not as comprehensive as a blanket ban. *Id*. at 878-79 (emphasis added).

Third, the district court found it "significant[]" that Microsoft's proposed alternative—notifying a senior official or U.S. lawyer at the company of the mere fact of the warrant, with additional disclosures to that individual subject to an appropriate protective order—"does not extinguish the burden on speech" but "simply shifts it to others." JA-93 n.7. That analysis is topsy-turvy—assuming that it is better for a company to be kept entirely in the dark about government surveillance of its confidential material than for the company to learn of the *fact* that a warrant has been served, at which point the company can decide whether to enter into an appropriate protective order so it can gain additional information needed to

protect its legal interests. Giving appropriate company personnel the opportunity to exercise the company's rights reduces the intrusion on constitutional protections.

Fourth, the court dismissed Microsoft's proposed alternatives as "impractical" (JA-94), and the Third Circuit committed a similar error in stating a court cannot "assess the trustworthiness of a would-be confidante chosen by a service provider." *Subpoena 2018R00776*, 947 F.3d at 159. But the Department of Justice has accepted a similar offer in recent litigation. *See* Microsoft Br. at 30. As just mentioned, strict scrutiny demands that the *government* show that it has considered whether a solution along these lines would be workable and, if not, meet its burden of explaining why the alternative will not provide sufficient protections for the government's interests.

Finally, although Microsoft requested access to the government's *ex parte* submissions, the court denied that request without explanation in a single sentence. *See* JA-92 n.4 ("Microsoft's request for access to the Government's ex parte affidavit in support of the warrant so that it can 'refute or explain why' the underlying facts 'have no bearing on the strict scrutiny analysis' (ECF No. 45 at 24-25) is denied."). The district court gave no reason why disclosure or summary of this information to Microsoft's *counsel*, with the requisite clearance or protections, would risk jeopardizing an ongoing investigation into Microsoft's *customer*—and none is apparent. "Only in the most extraordinary circumstances" do courts

"countenance [] reliance upon *ex parte* evidence to decide the merits of a dispute." *Abourezk v. Reagan*, 785 F.2d 1043, 1061 (D.C. Cir. 1986), *aff'd*, 484 U.S. 1 (1987).

By summarily denying the request for access, the district court forced Microsoft to argue against continued secrecy with both hands tied behind its back. As explained above in Part II.B, moreover, that decision not only put Microsoft at a severe disadvantage in challenging the gag order, but it deprived Microsoft's customer of a fair opportunity to learn about—and assert applicable rights or privileges in response to—the government's surveillance.

CONCLUSION

The Court should vacate the denial of Microsoft's motion to modify the secrecy order.

Dated: December 21, 2020

Respectfully submitted.

/s/ Andrew J. Pincus
Andrew J. Pincus
MAYER BROWN LLP
1999 K Street, NW
Washington, DC 20006
(202) 263-3000
apincus@mayerbrown.com

Counsel for Amici Curiae

Tara S. Morrissey
U.S. CHAMBER LITIGATION CENTER, INC.
1615 H Street, NW
Washington, DC 20062
(202) 463-5337

Counsel for the Chamber of Commerce of the United States of America

Re-Submitted: January 25, 2021

CERTIFICATE OF COMPLIANCE
WITH TYPEFACE AND WORD-COUNT LIMITATIONS

I hereby certify that this brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5); the type style requirements of Fed. R. App. P. 32(a)(6); and the type volume limitations of Fed. R. App. P. 29(a)(5) and 32(a)(7)(B) and L.R. 29.1(c) and 32.1(a)(4)(A), because it is proportionally spaced and has a typeface of 14-point Times New Roman, and contains 6,030 words, excluding the parties of the brief exempted by Fed. R. App. P. 32(f).

/s/ Andrew J. Pincus
Andrew J. Pincus

CERTIFICATE OF SERVICE

I hereby certify that on this 26th day of January, 2021, I electronically filed the foregoing with the Clerk of Court for the United States Court of Appeals for the Second Circuit by using the appellate CM/ECF system. I further certify that all participants in the case are registered CM/ECF users, who will be served by the appellate CM/ECF system.

/s/ Andrew J. Pincus
Andrew J. Pincus