No. 20-1474

IN THE

Supreme Court of the United States

JOSEPH COLONE,

Petitioner,

v.

THE SUPERIOR COURT OF THE
STATE OF CALIFORNIA,
FOR THE COUNTY OF SAN FRANCISCO,

Respondent.

GITHUB, INC.,

Real Party in Interest.

**On Petition For A Writ Of Certiorari
To The Supreme Court Of The State Of California**

BRIEF OF GITHUB, INC., IN OPPOSITION

W. Douglas Sprague
COVINGTON & BURLING LLP
Salesforce Tower
415 Mission Street
Suite 5400
San Francisco, CA 94105
(415) 591-6000
dsprague@cov.com

Alexander A. Berengaut
Counsel of Record
Megan A. Crowley
COVINGTON & BURLING LLP
One CityCenter
850 Tenth Street, NW
Washington, DC 20001
(202) 662-6000
aberengaut@cov.com
mcrowley@cov.com

QUESTION PRESENTED

The Stored Communications Act ("SCA") prohibits covered service providers from "knowingly divulg[ing] to any person or entity the contents" of their customers' electronic data held in storage, absent an applicable statutory exception. 18 U.S.C. § 2702(a).

The question presented is whether the SCA authorizes a petitioner in a post-conviction habeas proceeding to compel a covered service provider to disclose its customer's content data, where no statutory exception in the SCA would permit the disclosure.

CORPORATE DISCLOSURE STATEMENT

GitHub, Inc. is a wholly-owned subsidiary of Microsoft Corp.

TABLE OF CONTENTS

INDEX TO SUPPLEMENTAL APPENDIX

TABLE OF AUTHORITIES

Page(s)

Cases

Baldrige v. Shapiro,
455 U.S. 345 (1982)..25, 26

Barber v. Page,
390 U.S. 719 (1968)..26

In re Barnett,
31 Cal.4th 466 (2003).....................................10, 28

Cazorla v. Koch Foods of Miss., LLC,
838 F.3d 540 (5th Cir. 2016)................................24

Consumer Prod. Safety Comm'n v. GTE Sylvania, Inc., 447 U.S. 102 (1980)....................22

Crispin. v. Christian Audigier, Inc.,
717 F. Supp. 2d 965 (C.D. Cal. 2010).....11, 16, 19

In re England,
375 F.3d 1169 (D.C. Cir. 2004)......................23, 24

Facebook, Inc. v. Superior Ct.,
4 Cal. 5th 1245 (2018)..21

Facebook, Inc. v. Wint,
199 A.3d 625 (D.C. App. 2019) 12, 19, 24, 25

Gall v. Kentucky,
702 S.W.2d 37 (Ky. 1985)....................................28

In re Grothe,
208 N.E.2d 581 (Ill. App. 1965) 28

Hall v. United States,
566 U.S. 506 (2012) 18

Hartford Underwriters Ins. Co. v. Union Planters Bank, N.A., 530 U.S. 1 (2000) 21

Henson v. Santander Consumer USA Inc.,
137 S. Ct. 1718 (2017) 18

Hickey v. Comm'r of Corr.,
842 A.2d 606 (Conn. App. 2004) 28

Hilton v. Braunskill,
481 U.S. 770 (1987) 10

Lamie v. U.S. Tr.,
540 U.S. 526 (2004) 21

Layne & Bowler Corp. v. W. Well Works,
261 U.S. 387 (1923) 16

Maslenjak v. United States,
137 S. Ct. 1918 (2017) 16

Microsoft Corp. v. AT&T Corp.,
550 U.S. 437 (2007) 19

Mintz v. Mark Bartelstein & Assocs., Inc.,
885 F. Supp. 2d 987 (C.D. Cal. 2012) 11

The Monrosa v. Carbon Black Export, Inc.,
359 U.S. 180 (1959) 26

Sanchez v. State,
691 S.W.2d 795 (Tex. App. 1985) 27

St. Regis Paper Co. v. United States,
368 U.S. 208 (1961).......................................23, 24

State v. Bray,
422 P.3d 250 (Or. 2018) 12

In re Subpoena Duces Tecum to AOL, LLC,
550 F. Supp. 2d 606 (E.D. Va. 2008) 10, 20

Suzlon Energy Ltd. v. Microsoft Corp.,
671 F.3d 726 (9th Cir. 2011)...................11, 14, 21

Theofel v. Farey-Jones,
359 F.3d 1066 (9th Cir. 2004).......................13, 14

United States v. Gilman,
347 U.S. 507 (1954)...18

United States v. Hernandez,
913 F.2d 1506 (10th Cir. 1990)...........................15

United States v. Johnson,
529 U.S. 53 (2000)...22

United States v. Lorenzetti,
467 U.S. 167 (1984)...19

United States v. Nix,
251 F. Supp. 3d 555 (W.D.N.Y. 2017) 12

United States v. Pierce,
785 F.3d 832 (2d Cir. 2015) 12

Statutes

Other Authorities

Kenneth W. Graham, Jr., & Ann Murphy, *Federal Practice and Procedure* (1st ed. 2020) 15

Rebecca Wexler, *Privacy as Privilege: The Stored Communications Act and Internet Evidence*, 134 Harv. L. Rev. 2721 (2021)...................................13

S. Rep. No. 99-541 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555...3, 22

Stephen M. Shapiro et al., *Supreme Court Practice* (11th ed. 2019)...16, 26

INTRODUCTION

The SCA creates a comprehensive framework governing the privacy of electronic communications and other data stored online by cloud-based service providers like Real Party in Interest GitHub, Inc. As a general rule, the SCA prohibits providers like GitHub from disclosing the contents of their customers' data, except in limited exceptions prescribed by the SCA. Here, Petitioner argues that the lower courts should have disregarded the SCA's clear prohibition on disclosure and required GitHub to produce its customer's confidential and proprietary content data in response to Petitioner's subpoena, for use in Petitioner's post-conviction state habeas proceedings, even though none of the SCA's exceptions apply.

GitHub respectfully submits that the petition for a writ of certiorari should be denied. The issue Petitioner asks the Court to review—whether the SCA prohibits a service provider from disclosing its customer's content data outside the statute's carefully delineated exceptions—is not unsettled nor the subject of disagreement among the lower courts. To the contrary, every court to have considered the issue has rejected Petitioner's argument.

Petitioner nonetheless argues that the Court should grant the petition to address a purported conflict among lower courts regarding "implied statutory privileges" and whether the SCA "impliedly creates a novel, unqualified evidentiary privilege for the Internet." Pet. 14, ii. But Petitioner has not established that such a conflict exists, particularly because he fails to cite a single case adopting his novel interpretation of the SCA. Moreover, even if there were disagreement among the lower courts regarding the proper way to interpret statutory privileges in the abstract, this would present at most a methodological tension in the interpretation of a variety of federal statutes, not a meaningful conflict warranting this Court's review.

Petitioner and *amici* also argue that the petition should be granted because the SCA's prohibition against disclosure undermines the truth-seeking function of the courts, thereby harming "prosecutors, criminal defendants, civil litigants, and the public alike." Pet. 23; *see also* Brief of Legal Scholars & Scientists as Amici Curiae Supporting Petitioner at 3–4; Brief of the National Association for Public Defense et al. as Amici Curiae Supporting Petitioner at 2. The fair and effective functioning of the judicial system is indisputably an important interest—particularly in the context of a capital case, as here. But Petitioner and *amici*'s policy concerns regarding the SCA should be directed to Congress, which carefully crafted exceptions to the statute's prohibition on disclosure to balance privacy and data-access interests, and did not include any exception permitting Petitioner's subpoena. Determining whether to recognize a new exception to allow service providers to disclose data for use in post-conviction habeas proceedings is a job for Congress, not the courts.

Finally, this case is a particularly poor candidate for certiorari because the ruling below is amply supported by alternative grounds. In particular, Petitioner has not established that the disputed data is "necessary" to the state habeas proceedings, as required by California Penal Code § 1334.2. Instead, the record reflects that subpoenaing GitHub for its customer's data is *not* necessary because the data is available directly from the customer itself. As Petitioner has recognized, the customer has agreed to produce the data so long as Petitioner executes a routine non-disclosure agreement to protect the proprietary nature of the data at issue. In addition, the petition does not disclose that Petitioner also has brought an action against GitHub's customer in Ohio state court, and that an Ohio court has ordered the customer to produce the precise data at issue here—relief that, if upheld on appeal, would moot this action.

The petition should be denied.

STATEMENT

1. The SCA is part of the Electronic Communications Privacy Act, which Congress passed in 1986 "to protect privacy interests in personal and proprietary information." S. Rep. No. 99-541, at 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557. The statute protects "electronic communications," which Congress broadly defined to include "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce." 18 U.S.C. § 2510(12).

The SCA applies to two types of electronic service providers: those that provide data storage and processing services, referred to as "remote computing service[s]" or "RCS," *id.* § 2711(2), and those that provide communication services, referred to as "electronic communication[s] service[s]" or "ECS," *id.* § 2510(15). These categories are not mutually exclusive. A "single service provider may act as an ECS at times and an RCS at other times," and thus may be subject to the SCA for each type of service. *Vista Marketing, LLC v. Burkett*, 812 F.3d 954, 964 n.5 (11th Cir. 2016).

Under the SCA, covered service providers "shall not knowingly divulge to any person or entity the contents" of electronic communications held in storage. 18 U.S.C. § 2702(a); *see also id.* § 2510(8) (defining "content" as "any information concerning the substance, purport, or meaning of [an electronic] communication"); *id.* § 2510(12) (defining "electronic communication"). Congress codified the SCA in the federal criminal code and authorized significant liability for providers who knowingly violate the law. Any "person aggrieved by any violation" of the SCA can seek statutory damages, punitive damages, equitable relief, and attorneys' fees. *Id.* § 2707(a)–(c).

The SCA enumerates certain "[e]xceptions" to its ban on disclosure, under which providers "may divulge" the contents of a communication, *id.* § 2702(b)—for example, if the sender or recipient of the communication consents to disclosure, *id.* § 2702(b)(3). The SCA does not contain any exception allowing a provider to disclose content data in response to a petitioner's subpoena issued in post-conviction habeas proceedings, a civil subpoena more generally, or a subpoena issued by a defendant in a criminal proceeding.

2a. Real Party in Interest GitHub is a cloud-based development platform where people host and review computer code, manage projects, and build computer software. GitHub qualifies as an electronic communication service provider and/or remote computing service provider subject to the SCA. *See id.* §§ 2510(15), 2711(2).

GitHub maintains industry-leading privacy policies and devotes substantial resources to protecting its customers' data, including their confidential and proprietary computer source code. *See* GitHub Privacy Statement, https://docs.github.com/en/github/site-policy/github-privacy-statement (last visited Aug. 5, 2021). The data customers place in private repositories with GitHub remain the property of the customers, not GitHub. *See* GitHub Terms of Service at E(2), https://docs.github.com/en/github/site-policy/github-terms-of-service (last visited Aug. 5, 2021).

b. Petitioner is an inmate who was convicted and sentenced to death following a criminal trial in Texas state court. In connection with its investigation into possible post-conviction habeas claims on Petitioner's behalf, the Texas Office of Capital and Forensic Writs (OCFW) sought access to the source code for STRmix™, which is a probabilistic genotyping computer program that was used to analyze DNA evidence in Petitioner's prosecution. STRmix™ was developed and is owned by the Institute of Environmental Science and Research (ESR), a research institute owned by the government of New Zealand.

Petitioner initially sought the source code from ESR, which agreed to provide access so long as OCFW signed a non-disclosure agreement ("NDA"). OCFW refused, claiming that the terms of the proposed agreement were "onerous and unnecessary." Supp. App. 38a.[1] Instead of continuing to negotiate a mutually-acceptable non-disclosure agreement with ESR, Petitioner sought to compel GitHub to produce the STRmix™ source code, over ESR's objection.

3a. On January 3, 2020, the Texas court issued an order stating that the source code and other related items sought by Petitioner are "material and necessary for the administration of justice in this State." Supp. App. 1a. On January 31, 2020, the California Superior Court issued a subpoena to GitHub for the source code and related materials identified in the Texas order. Supp. App. 4a-9a.

Upon receipt of the subpoena, GitHub notified Petitioner that it "would not be able to produce that content without the account owner's [ESR] consent," but that ESR "could and should be able to produce that information." Supp. App. 18a. GitHub further explained that ESR "would be . . . best positioned to identify and produce the relevant source code from [its] private repositories," and that if Petitioner "believe[s] that the 'STRmix' source code is located in [ESR's] private storage, [his] subpoena should be directed to [ESR], not GitHub." Supp. App. 15a.

[1] Real Party in Interest GitHub's supplemental appendix is cited as "Supp. App. __." Petitioner's appendix is cited as "Pet. App. __."

Petitioner then filed a Motion to Compel Production of Records Pursuant to California Penal Code § 1334.2, seeking an order requiring GitHub to either (1) provide access to all materials in ESR's account and permit Petitioner's expert to identify the source code, or (2) "ask its client ESR to identify the source code so that [GitHub] provides access to only that material." Supp. App. 26a.

b. After learning of Petitioner's subpoena to GitHub, ESR reiterated that "[g]iven the proprietary nature of the source code . . . [ESR] object[s] to any review of the source code without a signed NDA." Supp. App. 11a. ESR underscored that it "certainly objects to any review conducted of any STRmix™ source code which may be hosted on the GitHub site." *Id.* ESR also explained that "[c]oming to agreement on the language of the NDA would be the most efficient way of getting the source code review conducted." *Id.*

ESR's counsel later sent Petitioner a letter reiterating ESR's "willing[ness] to continue negotiations on the terms of the Non-Disclosure and Confidentiality Agreement in an attempt to develop an agreement satisfactory to ESR, OCFW and its expert witness." Supp. App. 34a. The letter explains that, to ESR's counsel's "knowledge and belief, all the material being sought by the OCFW from ESR has been produced subject to a Protective Order in the Texas proceeding, with the sole exception being the review of the [requested] source code." Supp. App. 33a. The letter reiterates that "ESR stands ready to allow an examination of the [source code] provided that any reviewing expert executes an acceptable non-disclosure agreement containing terms establishing the manner of inspection." Supp. App. 34a.

The letter explains that Petitioner's expert has already executed a non-disclosure agreement in connection with his review of the source code in other criminal proceedings. *Id.* The letter expresses ESR's willingness to allow Petitioner's expert (1) to review the source code again if he agrees in writing to the same non-disclosure agreement to which he previously agreed, or (2) to testify in Petitioner's Texas proceeding based on his prior examination of the source code. *Id.* Alternatively, ESR offered to continue to negotiate the terms of a mutually-agreeable non-disclosure agreement. *Id.*

4a. After full briefing, the Superior Court heard oral argument on Petitioner's motion to compel. During argument, the court explained that "a subpoena is not enforceable if compliance would violate the SCA" and "any disclosure violates the SCA unless it falls within an enumerated exception to the general prohibition." Supp. App. 44a. The court further observed that this conclusion is consistent with "every court in the country to consider the issue," which have uniformly "concluded that the [SCA's] general prohibition on disclosure . . . appl[ies] to criminal defendants' subpoenas." Supp. App. 45a-46a.

The court rejected Petitioner's argument that because the SCA does not create an "evidentiary privilege," GitHub is required to produce ESR's source code. Supp. App. 45a. The court said that it was "perplexed" as to why Petitioner was "not willing to get the source code directly from its source, . . . ESR" by "enter[ing] into the non-disclosure agreement." Supp. App. 49a. The court further observed that GitHub is "just a service provider" "caught in the middle" between Petitioner and ESR, *id.*, and "[i]f [Petitioner] wishes to review the source code, he may do so by entering into the non-disclosure agreement required by ESR," Pet. App. 6.

The Superior Court then issued an order denying Petitioner's motion, concluding that "the subpoena Colone served on GitHub, Inc. is prohibited by the Stored Communications Act, and therefore must be quashed." Pet. App. 5.

b. Petitioner filed a petition for writ of mandate with the Court of Appeal, seeking an order directing the Superior Court to vacate its order, and compelling GitHub to produce ESR's data. Pet. App. 2. The Court of Appeal denied the petition, recognizing that "unanimous case authorities" prohibit entities like GitHub from divulging customer content data pursuant to a discovery request. Pet. App. 3.

c. Petitioner then filed a petition in the California Supreme Court, seeking review of the Court of Appeal's denial of his writ petition or, in the alternative, a writ of mandate compelling GitHub to produce ESR's source code. Pet. App. 1. The California Supreme Court denied discretionary review of the petition. *Id.*

5. In a separate proceeding in Ohio state court not mentioned in the petition, Petitioner served a subpoena seeking the STRmix™ source code from ESR's U.S.-based counsel. Supp. App. 59a. ESR's counsel filed a motion to quash the subpoena, which

was denied by the Court of Common Pleas in Summit County, Ohio, on March 11, 2021. *Id.* ESR's counsel filed an appeal, which is currently pending before the Ninth Judicial District of the Ohio Court of Appeals. Supp. App. 60a. The parties are currently participating in mediation, pursuant to the Court's order. *Id.*

REASONS FOR DENYING THE PETITION

I. There Is No Conflict In Authority.

Petitioner seeks review of an issue on which courts are in universal agreement: the SCA prohibits a service provider from disclosing its customer's content data outside the statute's carefully delineated exceptions, such as in response to a civil subpoena issued in connection with post-conviction habeas proceedings. *See* 18 U.S.C. § 2702(a).

As courts have uniformly concluded, the SCA's "plain and unambiguous language . . . prohibits an [ECS] or [RCS provider] from knowingly divulging to any person or entity the contents of customers' electronic communications or records." *In re Subpoena Duces Tecum to AOL, LLC*, 550 F. Supp. 2d 606, 609–10 (E.D. Va. 2008). And "it is plain that the SCA does not provide an exception to its general prohibition on disclosure for civil subpoenas." *PPG Indus., Inc. v. Jiangsu Tie Mao Glass Co.*, 273 F. Supp. 3d 558, 560 (W.D. Pa. 2017).[2] "Not only is such an exception not

[2] This Court's "decisions have consistently recognized that habeas corpus proceedings are civil in nature." *Hilton v. Braunskill*, 481 U.S. 770, 776 (1987); *see*

enumerated in the statute, but there is a seemingly settled body of decisional law that affirmatively states that civil subpoenas provide no such exception." *Id.* (citations omitted); *see also, e.g.*, *Mintz v. Mark Bartelstein & Assocs., Inc.*, 885 F. Supp. 2d 987, 991–92 (C.D. Cal. 2012) (similar); *Crispin. v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965, 975–76 (C.D. Cal. 2010) (similar); *Viacom Int'l Inc. v. Youtube Inc.*, 253 F.R.D. 256, 264 (S.D.N.Y. 2008) (similar).

Moreover, courts have widely recognized that "Congress' primary intent in passing the [SCA] was to protect the privacy interests of American citizens"—a goal that would be undermined if the courts were to craft a non-statutory exception to the SCA's ban on disclosure. *Suzlon Energy Ltd. v. Microsoft Corp.*, 671 F.3d 726, 730 (9th Cir. 2011) (citing S. Rep. No. 99–541, at 3–5); *Sams v. Yahoo! Inc.*, 713 F.3d 1175, 1179 (9th Cir. 2013) ("The SCA was enacted because the advent of the Internet presented a host of potential privacy breaches that the Fourth Amendment does not address."). As the Ninth Circuit has explained, "[d]eclaring an implicit exception to the [SCA] for civil litigation would erode the safety of the stored electronic information and trigger Congress' privacy concerns." *Suzlon*, 671 F.3d at 730; *see also O'Grady v. Superior Ct.*, 44 Cal. Rptr. 3d 72, 87 (Cal. App. 6th Dist. 2006), *as modified* (June 23, 2006) (SCA's legislative history "suggests an intent to protect the

also, e.g., *In re Barnett*, 31 Cal.4th 466, 478 n.10 (2003) ("[H]abeas corpus proceedings . . . are properly viewed as civil actions designed to overturn presumptively valid criminal judgments and not as part of the criminal process itself.").

privacy of stored electronic communications *except where* legitimate law enforcement needs justify its infringement").

Even if Petitioner's subpoena were construed as a request from a criminal defendant, as opposed to a civil litigant, there *still* would be no conflicting law warranting this Court's review, nor any applicable exception under the SCA permitting GitHub to disclose its customer's data. *See* 18 U.S.C. § 2702(b)(1)–(9) (no exception for subpoenas issued by criminal defendants). As the Superior Court correctly noted, "every court to consider the issue has concluded that the SCA's general prohibition on disclosure . . . applies to criminal defendants' subpoenas." Pet. App. 5–6. *See also Facebook, Inc. v. Wint*, 199 A.3d 625, 629 (D.C. App. 2019); *State v. Bray*, 422 P.3d 250, 256 (Or. 2018); *United States v. Pierce*, 785 F.3d 832, 842 (2d Cir. 2015); *United States v. Nix*, 251 F. Supp. 3d 555, 559 (W.D.N.Y. 2017); *United States v. Wenk*, 319 F. Supp. 3d 828, 829 (E.D. Va. 2017). Thus, there is no conflict among the lower courts for this Court to resolve.

Petitioner nonetheless argues that his petition should be granted because "the federal circuits and state high courts are split over whether ambiguous silence in the Stored Communications Act impliedly creates an unqualified evidentiary privilege for the Internet." Pet. 16. But Petitioner does not cite a single case in which any court has adopted this novel interpretation of the SCA. Indeed, a law review article on which Petitioner relies acknowledges that every court to have considered the issue has rejected Petitioner's argument. *See* Rebecca Wexler, *Privacy as*

Privilege: The Stored Communications Act and Internet Evidence, 134 Harv. L. Rev. 2721, 2724 (2021) ("For over a decade, federal and state courts across the country have construed the SCA to bar criminal defendants from subpoenaing technology companies for the contents of another's electronic communications.").

Citing *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2004), Petitioner nevertheless contends that the Ninth Circuit "recognized that the SCA does not bar non-governmental litigants from accessing stored electronic communications via a lawful subpoena." Pet. 18.

Theofel concerned Section 2701 of the SCA, which creates a private cause of action against anyone who "intentionally accesses without authorization a facility through which an electronic communication service is provided." 18 U.S.C. § 2701(a)(1). In *Theofel*, defendants were civil litigants who intentionally issued an overbroad subpoena for plaintiffs' emails, and the service provider—NetGate—produced hundreds of emails in response. The Ninth Circuit held that defendants violated Section 2701 by issuing a "transparently and egregiously" overbroad subpoena. *Theofel*, 359 F.3d at 1074. Contrary to Petitioner's suggestion, the court did not address NetGate's responsibilities under the SCA beyond noting that it had a "legal obligation not to disclose [email] messages to third parties." *Id.* (citing 18 U.S.C. § 2702(a)(1)).

In concluding that defendants violated Section 2701, the Ninth Circuit explained that the district court erred in holding that NetGate had consented to the disclosure of the emails. The Ninth Circuit explained that NetGate disclosed the emails "in response to defendants' purported subpoena," but "[u]nbeknownst to NetGate, that subpoena was invalid." *Id.* These facts, the Ninth Circuit held, "vitiate[d] NetGate's consent." *Id.* at 1073. And while the court noted that "[t]he subpoena's falsity transformed the access from a bona fide state-sanctioned inspection into private snooping," *id.*, the court did not conclude—as Petitioner asserts, Pet. 18—that if defendants had served NetGate with a valid subpoena, the disclosure would have been lawful. Rather, the court merely recognized that "Section 2701(c)(1) . . . provides no refuge for a defendant who procures consent by exploiting a known mistake that relates to the essential nature of his access." *Id.*

Accordingly, Petitioner's claim that the Ninth Circuit has held that the SCA permits compliance with civil subpoenas is incorrect. In fact, just the opposite is true: like every other court to address this issue, the Ninth Circuit concluded that the SCA *does not* contain an exception for civil subpoenas.

Nor has any court concluded that enforcing the plain language of the SCA implicitly creates an "evidentiary privilege," as Petitioner argues. Pet. 11–12. Rather, courts have widely recognized that the SCA sets forth a statutory framework prohibiting the disclosure of content data except in specific circumstances not applicable here. *See, e.g.*, *Suzlon*, 671 F.3d at 729 ("18 U.S.C. § 2702(b) and (c) list numerous exceptions to the rule as set forth in

§ 2702(a), which prohibits the knowing divulgence of the contents of a communication while in electronic storage."). Thus, the SCA does not function as a privilege that "'makes . . . information immune from process,'" Pet. 8 (quoting 23A Kenneth W. Graham, Jr., & Ann Murphy, *Federal Practice and Procedure* § 5437 (1st ed. 2020)); instead, it merely provides a framework through which private parties can obtain user content data if they satisfy one of the statutory exceptions to disclosure.

Lacking any authority supporting its interpretation of the SCA, Petitioner cites cases interpreting *other* federal statutes to argue that there is a "sharp conflict among the federal circuits over whether, or in what circumstances, courts may conclude that, despite facial silence regarding privilege, statutory language impliedly creates a privilege." Pet. 10. But courts in those cases concluded that preventing disclosure was inconsistent with the specific statutory framework and Congressional intent at issue. *See Zambrano v. INS*, 972 F.2d 1122, 1126 (9th Cir. 1992), *vacated on other grounds*, 509 U.S. 918 (1993) ("[p]roviding the names of class members to class counsel facilitates, rather than frustrates, the legislative intent of the statute"); *United States v. Hernandez*, 913 F.2d 1506, 1511 (10th Cir. 1990) (interpreting Immigration Reform and Control Act "in a manner which prohibited the Attorney General from disclosing that an illegal alien had applied for amnesty would frustrate the salutary policy behind [the statute]"); *In re Nelson*, 873 F.2d 1396, 1397 (11th Cir. 1989) ("There is no indication that Congress intended to prohibit disclosure of [Special Agricultural Worker] application files in judicial proceedings."). Here, by contrast, the SCA contains explicit language barring disclosure, which reflects Congress's "expressed intention" in enacting the SCA. *See Crispin*, 717 F. Supp. 2d at 975 (the SCA "is at heart a broad prohibition on disclosure with limited and carefully regulated exceptions").

In any event, even if Petitioner were correct that lower courts have differed in their analysis of evidentiary privileges across various federal statutes, these purportedly divergent approaches would present—at most—a methodological tension in judicial interpretation, not a "real and embarrassing conflict of opinion and authority between the [lower courts]" requiring this Court's review. *Layne & Bowler Corp. v. W. Well Works*, 261 U.S. 387, 393 (1923); *see also* Stephen M. Shapiro et al., *Supreme Court Practice* § 4.3 (11th ed. 2019) ("[For certiorari to be granted] there must be a real or 'intolerable' conflict on the same matter of law or fact, not merely an inconsistency in dicta or in the general principles utilized" (collecting cases)).

And this case presents a poor vehicle to address any such conflict. As explained above, courts have uniformly concluded that the SCA bars disclosure of content data outside the statute's enumerated exceptions, including in response to a civil subpoena. Accordingly, this Court does not have the full benefit of "the crucible of adversarial testing on which [it] usually depend[s]." *Maslenjak v. United States*, 137 S. Ct. 1918, 1931 (2017) (Gorsuch, J., concurring in part and concurring in the judgment). And to the extent the Court believes that it is important to consider the question of implied privileges, there are other cases percolating in the lower courts involving other statutes that would serve as better vehicles. *See* Pet. 27 ("At least six federal appellate courts have already deliberated, decided, and divided on the issue of whether, or in what circumstances, courts may construe ambiguous silence in statutory text as impliedly creating privilege."). Not one of those cases involves the unique language, structure, and purpose of the SCA.

II. Congress, Not The Judiciary, Is The Appropriate Branch To Address The Policy Concerns Petitioner Raises.

Petitioner next argues that his petition should be granted because the SCA's prohibition on disclosure "undermines judicial truth-seeking with no clear societal benefit." Pet. 24. Similarly, *amici* maintain that the SCA's prohibition on disclosure precludes Petitioner "from obtaining information crucial to assessing the fairness of his criminal trial . . . [and] impair[s] his ability to obtain remedies for companion fair trial rights." Brief of Legal Scholars & Scientists as Amici Curiae Supporting Petitioner at 4; *see also* Brief of the National Association for Public Defense et al. as Amici Curiae Supporting Petitioner at 2–3. While the circumstances under which habeas petitioners and criminal defendants can access evidence stored in the cloud is a substantial policy issue, Petitioner's policy concerns are not a basis for departing from the plain language of the SCA. Instead, Petitioner's policy concerns are properly addressed to Congress.

"[T]he proper role of the judiciary" is "to apply, not amend, the work of the People's representatives." *Henson v. Santander Consumer USA Inc.*, 137 S. Ct. 1718, 1726 (2017). Judicial restraint is particularly appropriate in this case, where Petitioner asks the Court to rebalance the interests of habeas petitioners and criminal defendants against the privacy interests of persons who host their data with providers like GitHub—a balance Congress already struck through the SCA's unambiguous text. *See Hall v. United States*, 566 U.S. 506, 523 (2012) ("Given the statute's plain language, context, and structure, it is not for us to rewrite the statute . . . ."). It is the role of Congress—not the courts—to balance these competing policy interests and craft appropriately tailored solutions to promote access to evidence with adequate regard for data security and privacy. *See Patsy v. Bd. of Regents of Fla.*, 457 U.S. 496, 513 (1982) (noting Congress's "superior institutional competence" on matters of policy); *United States v. Gilman*, 347 U.S. 507, 511–13 (1954) ("The selection of that policy which is most advantageous to the whole involves a host of considerations that must be weighed and appraised. That function is more appropriately for those who write the laws, rather than for those who interpret them.").[3]

[3] Nor does the SCA's prohibition on disclosure lack a "clear societal benefit," as Petitioner asserts. Pet. 24. Courts have widely recognized the privacy interests served by the SCA. For example, as the D.C. Court of Appeals explained, "channeling . . . discovery to senders or recipients, rather than providers, increases

Petitioner also argues that providers like GitHub have used the SCA to secure "a special exemption from the burdens of complying with judicial process that others must bear." Pet. 26. Yet as the Superior Court correctly recognized, GitHub is "just a service provider" "caught in the middle" between Petitioner and ESR, and GitHub must comply with the law as written. Supp. App. 49a. There is no question that the SCA is in some respects outdated—it was enacted in 1986 "prior to the advent of the Internet and the World Wide Web" and is "ill-suited to address modern forms of communication." *Crispin*, 717 F. Supp. 2d at 988. However, "[i]t is for Congress, not the courts, to revise longstanding legislation in order to accommodate the effects of changing social conditions." *United States v. Lorenzetti*, 467 U.S. 167, 179 (1984). Thus, any updates to the SCA must "be made after focused legislative consideration, and not by the Judiciary forecasting Congress' likely disposition." *Microsoft Corp. v. AT&T Corp.*, 550 U.S. 437, 459 (2007).

Moreover, deferring to Congress would not lead to the dire consequences Petitioner describes. Pet. 23. While habeas petitioners (and civil litigants more broadly) cannot obtain content data by serving civil discovery requests on service providers, they are free to direct such requests to the owners of the data

the chances that affected individuals can assert claims of privilege or other rights of privacy before covered communications are disclosed to criminal defendants in response to subpoenas." *Wint*, 199 A.3d at 631.

themselves (such as ESR), or any other party with access to the data that is not subject to the SCA. Indeed, that is exactly what Petitioner has done here, serving a subpoena on ESR for the STRmix™ source code, and securing a court order requiring ESR to "produce the STRmix source code for review by [Petitioner's] expert." Supp. App. 59a.

"The business of enacting statutory fixes [is] one that belongs to Congress and not this Court." *Perry v. Merit Sys. Prot. Bd.*, 137 S. Ct. 1975, 1988 (2017) (Gorsuch, J., dissenting). Petitioner's concerns with the existing law are not a basis to usurp Congress's role in deciding whether and when service providers should be authorized to disclose their customer's data.

III. The Lower Courts' Decisions Were Correct.

Petitioner argues that the Superior Court erred in denying his motion to compel, and the Court of Appeal and California Supreme Court compounded this error by failing to issue the extraordinary remedy of a writ of mandate. These purported errors are not a sufficient basis for certiorari for the reasons discussed above. But even if they were, there was no error in the lower courts' decisions.

A. The Superior Court Correctly Concluded That Petitioner's Subpoena Violates Federal Law.

It is undisputed that GitHub is subject to Section 2702(a) of the SCA, which "clearly prohibits any disclosure of stored [content data] other than as authorized by enumerated exceptions." *O'Grady*, 139 Cal. App. 4th at 1443; *In re Subpoena*, 550 F. Supp. 2d at 609–10; *see also* 18 U.S.C. § 2702(a). This statutory prohibition is subject to limited and narrow exceptions, 18 U.S.C. § 2702(b)(1)–(9), none of which allow a covered service provider to disclose its customer's content data in response to a civil subpoena issued in a state habeas proceeding.

Petitioner does not argue that his subpoena falls within one of the SCA's enumerated exceptions to disclosure. He nonetheless contends that the SCA does not prohibit GitHub from disclosing ESR's source code in response to Petitioner's subpoena, Pet. 17, 20—an argument that conflicts with the plain language of the statute and clearly-expressed Congressional intent.

"The starting point in discerning congressional intent is the existing statutory text . . . . '[W]hen the statute's language is plain, the sole function of the courts—at least where the disposition required by the text is not absurd—is to enforce it according to its terms.'" *Lamie v. U.S. Tr.*, 540 U.S. 526, 534 (2004) (quoting *Hartford Underwriters Ins. Co. v. Union Planters Bank, N.A.*, 530 U.S. 1, 6 (2000)). Here "there is no pertinent ambiguity in the language of the statute," *O'Grady*, 139 Cal. App. 4th at 1443: Congress plainly mandated that providers like GitHub may not disclose content data to "any person or entity"—subject to clear and comprehensive exceptions, none of which apply here.

This conclusion is consistent with Congress's intent in enacting the SCA: to protect "the privacy interests of American citizens," *Suzlon*, 671 F.3d at 730, and "avoid discouraging the use and development of new technologies," *Facebook, Inc. v. Superior Ct.*, 4 Cal. 5th 1245, 1289 (2018) (citing the SCA's legislative history). Thus, if Petitioner's argument were adopted, it would undermine the very interests that the SCA was designed to protect. *See also* S. Rep. No. 99–541, at 3.

Petitioner nonetheless argues that because the SCA "contains a plethora of exceptions that permit disclosures in a wide array of circumstances," the statute does not "impliedly creat[e] an unqualified evidentiary privilege that would bar criminal defendants' and other non-governmental litigants' so-ordered subpoenas." Pet. 31. As a threshold matter, the SCA does not operate as a privilege. The statute does not close all doors to *what* litigants can obtain, but only limits *from whom* they can obtain it, subject to certain specifically-enumerated exceptions permitting disclosure. Further, the fact that Congress crafted certain exceptions to the statutory bar on disclosure does not authorize the courts to imply an additional exception for civil subpoenas from habeas petitioners. To the contrary, "[i]f Congress had intended to exclude [civil subpoenas from habeas petitioners] from [the statutory restrictions,] it could easily have done so explicitly . . . as it did with respect to the other listed exceptions." *Consumer Prod. Safety Comm'n v. GTE Sylvania, Inc.*, 447 U.S. 102, 109 (1980). In short, "[w]hen Congress provides exceptions in a statute, it does not follow that courts have authority to create others." *United States v. Johnson*, 529 U.S. 53, 58 (2000).

Petitioner further argues that the Superior Court should have granted his motion to compel because, although the SCA expressly prohibits providers like GitHub from "divulg[ing content data] to *any person or entity*," 18 U.S.C. § 2702(a) (emphasis added), the statute does not specifically state that content data may not be disclosed in response to a civil subpoena from a habeas petitioner. Pet. 29. This Court "has repeatedly rejected such an approach to statutory construction." *In re England*, 375 F.3d 1169, 1179 (D.C. Cir. 2004) (collecting cases);[4] *see also, e.g.*, *PGA Tour, Inc. v. Martin*, 532 U.S. 661, 689 (2001) ("'[T]he fact that a statute can be applied in situations not expressly anticipated by Congress does not demonstrate ambiguity. It demonstrates breadth.'" (quoting *Pa. Dep't of Corrections v. Yeskey*, 524 U.S. 206, 212 (1998))).

Indeed, although "[c]ourts construing a federal statute have a 'duty to avoid a construction that would suppress otherwise competent evidence unless the statute, strictly construed, requires such a result," Pet. 30 (quoting *St. Regis Paper Co. v. United States*,

[4] Petitioner misstates the D.C. Circuit's decision in *In re England*, 375 F.3d 1169 (D.C. Cir. 2004), incorrectly claiming that the court "ruled that statutory language barring 'publication' does not create a privilege" against disclosure of information in civil litigation. Pet. 14–15. In fact, the D.C. Circuit held just the opposite, concluding that a statute that provided that certain Naval board proceedings "may not be disclosed to any person not a member of the board . . . block[s] civil discovery of [those] proceedings in civil litigation." *In re England*, 375 F.3d at 1181; *id.* at 1178 ("Disclosure of [the] proceedings in civil discovery would certainly undermine, if not totally frustrate, the purpose of [the statute].").

368 U.S. 208, 218 (1961)), courts have "appropriately rejected the theory that general language precluding disclosure will never suffice to preclude disclosure in response to subpoenas, and that only a specific statutory reference to subpoenas will suffice," *Wint*, 199 A.3d at 632 (collecting cases); *see also In re England*, 375 F.3d at 1181; *Cazorla v. Koch Foods of Miss., LLC*, 838 F.3d 540, 551 (5th Cir. 2016) ("[I]t is unclear why a provision broadly barring *any* 'disclosure' would have to specify 'including in discovery' in order to have effect.").

Nor do the cases cited by the Petitioner suggest otherwise. *See Pierce Cty., Wash. v. Guillen*, 537 U.S. 129, 144 (2003) (holding that "statutes establishing evidentiary privileges must be construed narrowly," taking into consideration the purpose of the statute, but *not* suggesting that Congress must use specific phrases in order to create a bar on discovery). Indeed, the principal cases on which Petitioner relies—*St. Regis Paper Co. v. United States* and *Baldrige v. Shapiro*—confirm the plain language interpretation of the SCA adopted by the courts below.

In *St. Regis*, this Court considered a provision of the Census Act that prohibited the Department of Commerce from "permit[ting] anyone other than the sworn officers and employees of the Department . . . to examine the individual [census] reports." 368 U.S. at 216 n.5 (1961). The Court concluded that this language—which, just like the SCA, did not explicitly mention civil discovery requests—barred discovery of census reports "while in the hands of . . . government officials." *Id.* at 218. Likewise, here, the SCA prohibits ECS and RCS providers like GitHub from "divulging [content data] to *any person or entity*," thereby prohibiting ECS and RCS providers from disclosing customer data in response to a civil discovery request. 18 U.S.C. § 2702(a) (emphasis added).

This Court's recognition in *St. Regis* that "the prohibitions against disclosure [in the Census Act] run only against the officials receiving such information," *St. Regis*, 368 U.S. at 217, does not suggest, as Petitioner asserts, that a party subject to express prohibitions against disclosure must respond to civil discovery requests. To the contrary, this Court concluded that a party subject to such prohibitions (whether the Commerce Department under the Census Act or GitHub under the SCA) *cannot* respond to such requests. *See id.* at 215–17 (the Commerce Department "is prohibited from using the information supplied for other than statistical purposes").

Similarly, in *Baldrige v. Shapiro*, 455 U.S. 345 (1982), this Court held that the Census Act's general prohibition on the disclosure of certain census data did *not* contain an implicit exception for civil discovery—a conclusion that refutes, rather than supports, Petitioner's arguments. As this Court explained, the Census Act's "strong policy of nondisclosure indicates that Congress intended the confidentiality provisions to constitute a 'privilege' within the meaning of the Federal Rules. Disclosure by way of civil discovery would undermine the very purpose of confidentiality contemplated by Congress." *Id.* at 361; *see also Wint*, 199 A.3d at 632 (citing *Baldrige* in support of the conclusion that the SCA prohibits RCS and ECS providers from responding to compulsory process).

B. Interpretation Of The SCA Is Not Dispositive To The Case.

In addition to the defects identified above, this case is a poor candidate for certiorari because the ruling below is amply supported by alternative grounds. In particular, Petitioner has not established that the disputed data is "necessary" to the state habeas proceedings, as required by California Penal Code § 1334.2. As a result, the interpretation of the SCA will ultimately be irrelevant to the outcome of this case, if the case were to be remanded. The Court routinely denies certiorari in such circumstances. *See, e.g.*, *The Monrosa v. Carbon Black Export, Inc.*, 359 U.S. 180, 183–84 (1959) (dismissing certiorari as improvidently granted because of alternative grounds for affirming lower court); Shapiro § 4.4(F) ("If the resolution of a clear conflict is irrelevant to the ultimate outcome of the case before the Court, certiorari may be denied.").

Section 1334.2 of the California Penal Code is California's codification of the Uniform Act to Secure the Attendance of Witnesses from Without a State in Criminal Proceedings ("Uniform Act"), which provides "a means by which prosecuting authorities from one State can obtain an order from a court in the State where the witness is found directing the witness to appear in the court in the first State to testify." *Barber v. Page*, 390 U.S. 719, 723 n.4 (1968). Before issuing a subpoena under Section 1334.2, a California court must hold a hearing and determine, *inter alia*, whether the requesting party has established that the witness is "material and necessary." Cal. Penal Code § 1334.2.

Here, Petitioner has not demonstrated—and cannot demonstrate—that subpoenaing GitHub is "necessary," because the data is available through other means. *See Sanchez v. State*, 691 S.W.2d 795, 796 (Tex. App. 1985) (petitioner did not establish necessity of testimony under Uniform Act where he had not established that "comparable testimony was not available from other sources"); *People v. Cavanaugh*, 69 Cal.2d 262, 271 (Cal. 1968) (cumulative testimony is not "necessary" for purposes of Section 1334). As noted, Petitioner served a subpoena on ESR's U.S.-based counsel, seeking the same data at issue here. On March 11, 2021, an Ohio court denied ESR's counsel's motion to quash the subpoena, and ordered ESR's counsel to "produce the STRmix source code for review by Mr. Colone's expert." Supp. App. 59a. That order is currently on appeal, and the parties are in mediation. Supp. App. 60a. If the Ohio court's order is upheld on appeal or the parties successfully mediate the matter, it would moot this action.

Even setting the Ohio proceedings aside, as Petitioner has acknowledged, ESR is willing to voluntarily provide access to the STRmix™ source code so long as Petitioner's expert witness signs a mutually-acceptable non-disclosure agreement, under terms the expert previously agreed to in another case. Supp. App. 34a. There is no indication in the record that Petitioner has exhausted this alternative pathway of obtaining the sought-after data.[5]

[5] The relief Petitioner seeks has two additional flaws under Section 1334.2. First, by its terms, Section 1334.2 authorizes a court to compel testimony for use in "prosecution[s]," and "grand jury investigation[s]." Cal. Penal Code § 1334.2. The *habeas* proceeding at issue here is neither. *See In re Barnett*, 31 Cal.4th at 478 n.10 (habeas corpus proceedings are civil actions); *Hickey v. Comm'r of Corr.*, 842 A.2d 606, 615 (Conn. App. 2004) (because habeas proceedings are civil in nature, the Uniform Act does not apply); *Gall v. Kentucky*, 702 S.W.2d 37, 45 (Ky. 1985) (same). Second, Section 1334.2 authorizes courts to compel testimony of out-of-state witnesses—not to require the production of documents, as Petitioner seeks here. *See Sams v. Yahoo!, Inc.*, No. CV-10-5897-JF (HRL), 2011 WL 1884633, at *4 n.5 (N.D. Cal. May 18, 2011), *aff'd* 713 F.3d 1175 (9th Cir. 2013). The impropriety of using Section 1334.2 to secure documents is even more apparent here, where the requested source code does not belong to GitHub. *See In re Grothe*, 208 N.E.2d 581, 586 (Ill. App. 1965) (using Uniform Act to obtain documents that "are not the property of the respondent" would be "manifestly inconsistent with the general purpose" of the Act).

CONCLUSION

For the reasons set forth above, the petition for a writ of certiorari should be denied.

Respectfully submitted,

ALEXANDER A. BERENGAUT
MEGAN A. CROWLEY
COVINGTON & BURLING, LLP
One City Center
850 Tenth Street, NW
Washington, DC 20001
Telephone: (202) 662-6000
Facsimile: (202) 662-6291
aberengaut@cov.com
mcrowley@cov.com

W. DOUGLAS SPRAGUE
COVINGTON & BURLING LLP
Salesforce Tower
415 Mission Street
Suite 5400
San Francisco, CA 94105
Telephone: (415) 591-6000
Facsimile: (415) 591-6091
dsprague@cov.com

August 6, 2021