IN THE SUPREME COURT OF THE STATE OF OREGON

STATE OF OREGON, Plaintiff-Adverse Party, v. DAVID AYON-URBANO, Defendant-Relator.	Marion County Circuit Court Case No. 24CR31979 S072084 MANDAMUS PROCEEDING
DAVID AYON-URBANO, Plaintiff-Relator, v. META PLATFORMS, INC., Defendant-Adverse Party.	Marion County Circuit Court Case No. 24CN05648 S072084 MANDAMUS PROCEEDING

BRIEF OF AMICI CURIAE LAW PROFESSORS IN SUPPORT OF DEFENDANT-RELATOR DAVID AYON-URBANO

Proceeding in Mandamus from the Order
of the Marion County Circuit Court
Honorable Jennifer Gardiner, Judge

DEAN ERWIN CHEMERINSKY
UC Berkeley School of Law

PROFESSOR REBECCA WEXLER
Columbia Law School

CHESA BOUDIN
Executive Director, Criminal Law & Justice Center
UC Berkeley School of Law

DANIEL A. RAYFIELD #064790
Attorney General
BENJAMIN GUTMAN #160599
Solicitor General
LEIGH SALMON #054202
Assistant Attorney General
400 Justice Building
1162 Court Street NE
Salem, OR 97301
(503) 378-4402

Leigh.a.salmon@doj.oregon.gov

Attorneys for Plaintiff-Adverse Party
State of Oregon

LINDSEY BURROWS #113431
Burrows Appellate Law LLC
333 SW Taylor St, Suite 300
Portland, OR 97204
(503) 882-4575
lindsey@burrowsappellatelaw.com

Attorneys for *Amici Curiae*
Law Professors

RIAN PECK, OSB 144012
Visible Law LLC
333 SW Taylor St, Suite 300
Portland, OR 97204
(503) 773-0130
rian@visible.law

ZACHARY STERN, OSB 134967
1900 Hines St SE, Ste 100
Salem, OR 97302
(503) 673-6736
zstern@zstern.com

GINGER MOONEY, OSB 031261
1017 May St, Ste 200
Hood River, OR 97301
(541) 716-5650
contact@mooneylaw.org

Attorneys for Defendant-Relator
David Ayon-Urbano

SARAH J. CROOKS, OSB 971512
SCrooks@perkinscoie.com
MATTHEW MERTINS, OSB 146288
MMertens@perkinscoie.com
1120 NW Couch St, 10th Floor
Portland, OR 97209
(503) 727-2000

Attorneys for Defendant-Adverse
Party
Meta Platforms, Inc.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Constitutional Provisions and Statutes

Other Authorities

AMICI CURIAE BRIEF OF LAW PROFESSORS

INTEREST OF AMICI CURIAE

We are a group of concerned law professors who teach, write, and research in the areas of constitutional law, evidence law, privacy law, criminal law, criminal procedure, civil procedure, and other subjects related to this case. Accordingly, we have a strong interest in the correct interpretation of federal preemption and evidentiary privilege doctrines that govern when federal statutes may preempt the compulsory process powers of Oregon courts. We recognize that the present matter will resolve important questions about whether the Stored Communications Act preempts the carefully crafted balance that Oregon law has set between society's truth-seeking interests in enabling criminal defendants to access evidence that is relevant to their defense and countervailing interests in keeping certain categories of information secret from judicial compulsory process.[1]

1. Chesa Boudin is the Executive Director of the Criminal Law and Justice Center at the University of California, Berkeley, School of Law.

[1] This brief was prepared by *amici curiae*. No counsel for any party authored this brief in whole or in part, and no monetary contribution was provided for preparation or submission of the brief. Institutional affiliations of *amici curiae* are included for identification purposes only.

2. Erwin Chemerinsky is the Dean and Jesse H. Choper Distinguished Professor of Law at the University of California, Berkeley, School of Law.
3. Jeffrey A. Fagan is the Isidor and Seville Sulzbacher Professor of Law at Columbia Law School.
4. Eric Fish is Acting Professor of Law at the University of California, Davis, School of Law.
5. Daniel Fryer is Assistant Professor of Law and Philosophy at the University of Michigan Law School.
6. Brandon L. Garrett is the L. Neil Williams, Jr. Distinguished Professor of Law at Duke University School of Law.
7. Ann M. Murphy is Professor of Law at the Gonzaga University School of Law.
8. Erin Murphy is the Norman Dorsen Professor of Civil Liberties at the New York University School of Law.
9. Alexander Nunn is Associate Professor of Law at the Texas A&M University School of Law.
10. Anna Roberts is Professor of Law at Brooklyn Law School.
11. Jeff Selbin is the Chancellor's Clinical Professor of Law at the University of California, Berkeley, School of Law.

12. Elisabeth Semel is the Chancellor's Clinical Professor of Law at the University of California, Berkeley, School of Law.
13. Jonathan Simon is the Lance Robbins Professor of Criminal Justice Law at the University of California, Berkeley, School of Law.
14. Olivier Sylvain is Professor of Law at the Fordham University School of Law.
15. Rebecca Wexler is the Alfred W. Bressler Professor of Law at Columbia Law School.

ISSUE PRESENTED

Does the Stored Communications Act (18 USC § 2702(a)) absolutely bar Oregon courts from enforcing a criminal defendant's subpoena, issued pursuant to ORS 136.580, for electronic communications contents stored by service providers such as Defendant-Adverse Party, Meta Platforms, Inc.?

ARGUMENT

I. Introduction

Oregon law recognizes the importance of criminal defendants being able to subpoena witnesses and the evidence that is necessary for their defense. *See, e.g.,* ORS 136.555-ORS 136.603. It would be wrong for a person to face conviction simply because there was not access to necessary evidence. Indeed, for courts to fulfill their mission of providing fair trials, full disclosure of facts is essential. *See*

State v. Cartwright, 336 Or 408, 417, 85 P3d 305 (2004) ("[W]hatever the scope of a court's authority [to grant a motion to quash a subpoena], such authority cannot permit trial courts to violate a criminal defendant's broad right under the subpoena statutes to compel witnesses to attend his or her trial (and to bring along any 'books, papers or documents' that the defendant has identified in the subpoena).").

Of course, there can be limits on access to information by criminal defendants and courts, such as when there is a legal privilege that prevents disclosure. *State v. Bray*, 363 Or 226, 269, 231, 422 P3d 250 (2018). For example, in *Bray*, this court recognized that a criminal defendant's subpoena for data contained on computers presents "risks to individual privacy," obligating this court to "adopt rules to protect against those risks." *Id.* Accordingly, in *Bray*, this court held that subpoenas *duces tecum* for computers containing digital data are subject to the same or similar particularity requirements as warrants. *Id.* (importing Article I, section 9, particularity analysis outlined in *State v. Mansor*, 363 Or 185, 208, 421 P3d 323 (2018) to subpoenas for digital data). This court explained that such protections are sufficient when the "only objection to a forensic examination is a generalized privacy objection and not a particularized objection based on a recognized privilege or statutory grant of confidentiality." *Bray*, 363 Or at 253.

This case poses the question of whether a federal statute, the Stored Communications Act, bars criminal defendants from having access to needed

information, even when a subpoena requires *in camera* review and satisfies the additional protections for digital privacy that this court set out in *Bray*. In *Bray*, this court stated that, under the Stored Communications Act, "[a] person like defendant, who is a nongovernmental entity, cannot require a remote computing service, such a Google, to divulge the contents of communications." *Id.* at 231 (citing 18 USC § 2703(b)). But this court did not further analyze the statute or consider preemption principles. *Amici* respectfully ask this court to revisit that interpretation and hold that the Stored Communications Act does not require a trial court to quash a criminal defendant's subpoena seeking *in camera* review.

Quite importantly, the Stored Communications Act is totally silent about how it applies in such circumstances and whether it was meant to supersede Oregon law. In light of this silence, it cannot be said that the Stored Communications Act preempts Oregon law on criminal defense subpoenas. There is nothing in the law or its legislative history that indicates that the Act is meant to preempt state laws in such circumstances. There thus is nothing to overcome the presumption against finding preemption. *Emerald Steel Fabricators v. Bureau of Labor and Industries*, 348 Or 159, 172-73, 230 P3d 518 (2010) (explaining presumption against preemption).

Moreover, in *St. Regis Paper Company v. United States* 368 US 208, 82 S Ct 289, 7 L Ed 2d 240 (1961), the Supreme Court held that federal laws should not be

read to overcome a right to compulsory process unless, strictly construed, they require such a result. The Stored Communications Act nowhere does this. *See generally*, Rebecca Wexler, *Privacy as Privilege: The Stored Communications Act and Internet Evidence*, 134 Harv L Rev 2721 (2021).

In light of the silence of the Stored Communications Act and the presumption against preemption, Oregon should follow its usual rules of evidence and procedure when evaluating the validity of a subpoena in this context. The trial court erred by quashing the subpoena under the Stored Communications Act.

II. Oregon Law Entitles Criminal Defendants to Subpoena Relevant Evidence and Appropriately Balances the Subpoena Power Against Competing Values.

Oregon law appropriately balances society's interests in criminal defense subpoenas that serve accuracy and fairness in criminal cases with competing interests in third-party privacy. This court should construe the Stored Communication Act's ("SCA's") ambiguous silence on criminal defense subpoenas as consistent with Oregon's carefully crafted criminal procedures. The SCA should not be read as an unqualified, absolute bar on criminal defense subpoenas for information that happens to be transmitted over the Internet.

A. Oregon Law Properly Balances Defense Access and Countervailing Interests in Secrecy.

Oregon law recognizes that criminal defendants must be able to access evidence that is relevant to their defense to safeguard the truth-seeking process of

the courts and the fairness of criminal proceedings. In particular, ORS 136.567 grants a criminal defendant the broad right to subpoena witnesses, and ORS 156.580 extends that right to subpoenas for "books, papers or documents." *See also Cartwright*, 336 Or at 413 (providing overview of statutory subpoena power for criminal defendants). As this court has emphasized, "[t]he very integrity of the judicial system and public confidence in the system depend on full disclosure of all the facts, within the framework of the rules of evidence." *Bray*, 363 Or at 251 (quoting *United States v. Nixon*, 418 US 683, 709, 94 S Ct 3090, 41 L Ed 2d 1039 (1974)). The defense subpoena statutes "ha[ve] constitutional dimensions," grounded in Article I, section 11, of the Oregon Constitution and the Fifth and Sixth Amendments to the United States Constitution. *Id.* "Courts must vindicate those guarantees, and 'to accomplish that it is essential that all relevant and admissible evidence be produced.'" *Bray*, 363 Or at 251 (quoting *Nixon*, 418 US at 711).

Oregon law also recognizes that the right to subpoena evidence is not absolute, and it establishes safeguards to balance the interests in truth-seeking and fairness that the subpoena process serves against competing interests, including privacy. For instance, Oregon law requires mandatory *in camera* review and, where appropriate, the imposition of protective measures as to specified evidence when subject to a defense subpoena. *See State ex rel Dugan v. Tiktin*, 313 Or 607,

609, 837 P2d 959 (1992) ("In Oregon, when an accused in a criminal case seeks pretrial access to a Children's Services Division (CSD) file made confidential under certain circumstances by statute, the trial court, upon a showing of good cause for disclosure, has a statutory duty to examine the file *in camera* to determine whether it contains information to which the defense is entitled." (citing ORS 135.873) (footnotes omitted)). In addition, ORS 135.873(2)[2] allows a court, upon good cause, to enter a protective order or otherwise restrict access to any other sensitive or confidential materials identified by the parties or "make any such order as is appropriate."

In *Cartwright*, this court provided an overview of the statutory subpoena power for criminal defendants. 336 Or at 413-18. This court explained that Oregon law does not expressly provide a mechanism for a motion to quash a defense subpoena. *Id.* at 417. "However, courts regularly receive and rule on motions to quash, and, whatever the scope of a court's authority in such circumstances, such

---

[2] ORS 135.873 provides, in pertinent part,

> "(2) Upon a showing of good cause, the court may at any time order that specified disclosures be denied, restricted or deferred, or make such other order as is appropriate.
>
> "(3) Upon request of any party, the court may permit a showing of good cause for denial or regulation of disclosures, or portion of such showing, to be made in camera. A record shall be made of such proceedings."

authority cannot permit trial courts to violate a criminal defendant's broad right under the subpoena statutes to compel witnesses to attend his or her trial (and to bring along any 'books, papers or documents' that the defendant has identified in the subpoena)." *Id.* When faced with a question of privilege or confidentiality as to subpoenaed materials, a trial court should conduct *in camera* review to evaluate "the *potential* uses of the subpoenaed material at trial, and, unless it is clear that the material or testimony has no potential use at trial, the court must deny the motion to quash." *Id.* at 419 (emphasis in original).

This court has specifically tailored that analysis to concerns regarding digital privacy. *Bray*, 363 Or at 252. The court has "recognized that a broad search of a personal computer may present risks to individual privacy similar to those presented by general warrants, and [the court, in *Mansor*,] adopted rules specific to such searches to ensure that an individual's right to computer privacy is adequately protected." *Id.* In *Bray*, the court further recognized that subpoenas for digital evidence "present[] similar risks to individual privacy." *Id.* Accordingly, this court determined that it had a "similar obligation to adopt rules" governing defense subpoenas "to protect against those risks." *Id.* This court adopted the following test specific to subpoenas for computers in order to protect digital privacy:

> "In *Mansor*, one of the rules that we adopted requires the party seeking to examine a computer to describe with particularity 'what' the party seeks to find and the temporal limitations if relevant and available. We also imposed limits on the use of information disclosed

> in the examination; a search is limited to the information identified in the warrant unless some warrant-exception applies. Similar rules are appropriate in this context. When a party is entitled to enforcement of a trial subpoena *duces tecum* for a witness's computer and its digital contents, the court must ensure that the forensic examination is reasonable and that only the digital information that was identified as potentially relevant to the cross-examination of that witness is disclosed to the parties and admitted."

Id. at 252-53.

This court explained that those protections are sufficient to protect against privacy-based objections to the disclosure of evidence. *Id.* at 253 ("If a witness's only objection to a forensic examination is a generalized privacy objection and not a particularized objection based on a recognized privilege or statutory grant of confidentiality, then those rules, as articulated in *Mansor*, should be sufficient to protect against an invasion of the witness's privacy."). And if there are additional objections based on privileges or statutory confidentiality, then courts should apply the familiar procedures allowing for *in camera* review and disclosure, when necessary. *Id.* ("If, however, the witness contends that the computer contains privileged information or information statutorily protected from disclosure, further protections, such as *in camera* inspection to ensure that privileged or statutorily protected information is not released, may be warranted.").

Through all these procedures, Oregon law sets a nuanced balance between protecting privacy interests and the need to accomplish the paramount goal "that

all relevant and admissible evidence be produced.'" *Id*. at 251 (quoting *Nixon*, 418 US at 711).

B. Construing the SCA as an Absolute Bar on Defense Subpoenas Would Make Meaningful Defense Investigation Impossible in Many Cases.

Construing ambiguous silence in the SCA's text as conflicting with Oregon's well-balanced laws and gutting the subpoena power would make meaningful defense investigation impossible in a growing percentage of cases. Criminal defendants need to subpoena third-party communications in a variety of circumstances. Such communications can be crucial for investigations into self-defense. They can also be essential to prove third-party guilt by identifying a true perpetrator. They also provide other forms of exculpatory evidence. For instance, a complaining witness's social media posts might prove that the person still possesses property that a defendant has been charged with stealing. Alternately, a third-party eyewitness's communications might offer a narration of events that corroborates that of the defense. Third-party communications can also be crucial for investigating witness bias and other credibility problems. Indeed, as society relies more and more on digital technologies, this essential evidence increasingly takes the form of electronic communications stored with service providers such as Meta. Denying defendants access to it threatens "the demise of due process and accurate fact-finding." (Erin Murphy, *Digital Evidence Generated by Consumer*

Products: The Defense Perspective, in *Human-Robot Interaction in Law and its Narratives: Legal Blame, Procedure, and Criminal Law*, 196 (2024)).

Crucially, it is often the case that the *only* way criminal defendants can obtain this essential evidence is by subpoenaing it from service providers such as Meta. Criminal defendants cannot rely on discovery from the government to obtain this type of evidence because the government may not possess it. Nor may they compel the state to obtain it for them, as this court has expressly held. *Bray*, 363 Or at 236-38. And the defense theory of the case may differ from that of the government such that the evidence falls outside the scope of the government's own investigation. In such circumstances, the government is under no obligation to investigate on behalf of the defense and cannot be conscripted into doing so. *Id*. On the contrary, in our adversarial system of justice, criminal defense lawyers are the sole actors tasked with finding exculpatory evidence that is not already possessed by the prosecution team. If defense lawyers do not get this evidence, no one will.

Although in some cases criminal defendants may be able to obtain this evidence by subpoenaing individual account holders directly, in many cases that is impossible. Account holders may be unreachable because they are deceased, because they are impossible to locate, because they reside abroad beyond the jurisdiction of courts within the United States, or because they assert an Article I,

section 12, or Fifth Amendment privilege against production. Account holders may also be unreliable sources of evidence because they refuse to comply with subpoenas or because there is a risk that they will destroy or tamper with the evidence. In some cases, subpoenaing an account holder would create a risk of flight. In other cases, account holders are dangerous and subpoenaing them would risk witness intimidation or a threat to someone's life or safety.

Therefore, in an increasing number of cases, the *only* way for criminal defendants to obtain essential evidence of third-party communications is by subpoenaing service providers such as Meta. If the ambiguous silence in the SCA's text were interpreted as an absolute bar on such subpoenas, then people would face conviction simply because they lack access to the evidence necessary to defend themselves. The result would be more wrongful convictions of factually innocent persons, more ineffective assistance of counsel, and less public trust in the justice system. In a world increasingly reliant on technological forms of proof, creating an absolute bar on defense access to critical evidence simply because it happens to be stored by a social media company "fatally undermines the presumption of innocence and the basic precepts of due process." Murphy, *Digital Evidence*, *supra* at 194.

There is no good reason to construe the SCA's ambiguous silence in this harmful way because Oregon's usual rules of evidence and procedure already

properly balance the competing interests at stake when criminal defendants subpoena sensitive information. Oregon's criminal procedures appropriately govern the disclosure of private information to criminal defense teams in thousands of cases each year. Oregon's criminal procedures successfully resolve conflicts between truth-seeking, fairness, and privacy for information that is far more sensitive than the vast majority of social media posts, including mental health and other medical records, personal diaries, financial data, location information, educational records, letters to loved ones, and more. And Oregon's criminal procedures will continue to successfully balance the competing interests at stake in criminal defense subpoenas for social media evidence without Meta's extreme interpretation of the SCA.

III. The SCA is Ambiguously Silent as to its Effect on Criminal Defense Subpoenas, so this Court Should Interpret the SCA to be Consistent with Oregon Law.

The SCA is ambiguously silent as to its effect on subpoenas requested by criminal defendants. Meta's claim to the contrary runs counter to the presumption against federal preemption, contradicts United States Supreme Court guidance to narrowly construe federal statutes as *not* blocking the truth-seeking process of courts, and distorts the SCA's textual silence into an implied, unqualified, absolute bar on criminal defense subpoenas for relevant evidence simply because that evidence was transmitted via the Internet. In effect, Meta is asking this court to

create an unconditional block on lawful judicial process based on a federal law that is totally silent on access to information by criminal defendants. This court should decline the invitation and instead maintain Oregon's well-crafted procedures for balancing society's interests in the enforcement of criminal defense subpoenas against overriding needs for secrecy.

A. The SCA's Text is Ambiguous.

The SCA states in relevant part:

> "Voluntary disclosure of customer communications or records
>
> "(a) Prohibitions.—Except as provided in subsection (b) or (c)—
>
> "(1) a person or entity providing an electronic communication service to the public ***shall not knowingly divulge*** to any person or entity the contents of a communication * * *."

18 USC § 2702(a) (emphasis added.)

It is ambiguous whether Congress intended the word "*divulge*" in section 2702(a) to refer to compliance with court-ordered judicial compulsory process and, in particular, with the type of *in camera* review procedure indicated by Oregon law when privacy interests and sensitive information are at stake. ORS 135.873. Webster's defines "divulge" as: "to make known" or "to make public." *Webster's Third New Int'l Dictionary* 664 (unabridged ed 2002). Meta's compliance with Mr. Ayon-Urbano's subpoena by submitting documents to a court in a limited and controlled manner, pursuant to a court order, for the purpose of enabling the court

to conduct *in camera* review, would not make anything "known" or "public." *See* ER-13 (subpoena *duces tecum* requiring Meta to submit documents for *in camera* review).

Indeed, courts conduct *in camera* review precisely to *prevent* information from being divulged unnecessarily. Hence, trade secret owners do not 'divulge' their intellectual property when they submit it to a court for *in camera* review. On the contrary, the trade secrets remain valid because submitting them to a court for *in camera* review does not make the information "generally known to the public or to other persons" but rather "preserve[s] the secrecy of [the] alleged trade secret by reasonable means[.]" ORS 646.469. Similarly, public officials do not 'divulge' anything when they submit records to a court for *in camera* review to determine whether those records should be made public. ORS 192.431. Nor do the Department of Human Services or other entities when required to submit confidential records for *in camera* review. *See, e.g.* ORS 409.225(1) (making DHS records pertaining to an individual child, family, or other recipient of services confidential); ORS 135.873 (providing procedures for *in camera* review for records subject to disclosure).

In each of these examples, complying with a court order to undertake the secure and trusted process of *in camera* review is the opposite of 'divulging' information. Records that do not contain relevant or essential evidence are shielded

from disclosure. *Cartwright*, 336 Or at 413-19. And, with criminal defense subpoenas, if the court decides that information must be shared with opposing counsel, then discretionary protective orders, sealing orders, and courtroom closures can prevent follow-on disclosures. *Id.*; ORS 135.873. Far from 'divulging' anything, procedures such as that contemplated by *Cartwright* and ORS 135.873 are designed to keep information *secret*.

Confidentiality provisions in federal statutes come in three categories: those that expressly block judicial compulsory process, those that expressly subject information to judicial compulsory process, and those that are textually silent on the matter and therefore ambiguous as to their effect on judicial compulsory process. The SCA falls into the third category, so its effect on criminal defense subpoenas is not mentioned in the law.

Congress knows how to block valid legal process when it wants to do so. Multiple federal statutes expressly privilege or exempt information from judicial compulsory process. *See, e.g.*, 5 USC § 574(a) (covered possessor of information "shall not voluntarily disclose or through discovery or compulsory process be required to disclose"); 23 USC § 407 (covered information "shall not be subject to discovery"); 13 USC § 9(a) (covered information "shall be immune from legal process"); 15 USC § 2055(e)(2) (covered information "shall be immune from legal process and shall not be subject to subpoena or other discovery"); 22 USC

§ 3144(d) (2000) (covered information "shall be immune from legal process"); 49 USC §§ 6307(b)(2)(B)(i)-(ii) (covered information "shall be immune from legal process"); 42 USC § 1395kk(e)(4)(D) (covered information "shall not be subject to discovery"); 42 USC § 299b-22(a) (covered information "shall be privileged and shall not be—(1) subject to a Federal, State, or local civil, criminal, or administrative subpoena * * *"); 15 USC § 7215(b)(5)(A) (covered information "shall not be subject to civil discovery or other legal process"); 23 USC § 148(h)(4) (covered information "shall not be subject to discovery"); 20 USC § 9573(d)(1)(B) (covered information "shall be immune from legal process"); 34 USC § 20110(d) (covered information "shall be immune from legal process"); 10 USC § 613a(b) (covered information is "immune from legal process"); 26 USC § 7525(a) (covered information is protected "to the extent the communication would be considered a privileged communication if it were between a taxpayer and an attorney").

As these examples show, Congress has many ways of expressly blocking judicial compulsory process and does so regularly. No "magic words" are necessary. Congress can and does use any number of express phrases to unambiguously bar subpoenas. It chose not to use such language in the SCA.

Congress also knows how to subject information to valid legal process when it wants to do so. To start, Congress has enacted a detailed legislative scheme—

promulgated by the Judicial Conference of the United States, approved by the United States Supreme Court, and reviewed by Congress pursuant to the Rules Enabling Act—that expressly regulates how criminal and civil litigants in federal court may subpoena information possessed by third parties. *See* FRCrP 17(c)(1), ("A subpoena may order the witness to produce any books, papers, documents, data, or other objects the subpoena designates."); FRCP 45(a)(1)(A)(iii) (a subpoena may "command each person to whom it is directed to * * * produce designated documents, electronically stored information, or tangible things in that person's possession * * *."). Those statutes set the general rule that all information is subject to valid subpoenas by default. In addition, Congress sometimes alters those default subpoena rules through confidentiality statutes that expressly subject certain information to customized forms of legal process. *See, e.g.*, 8 USC § 1202(f) (covered information "may be made available to a court which certifies that the information contained in such records is needed by the court in the interest of the ends of justice in a case pending before the court"). Once again, Congress chose not to use such language in the SCA.

In contrast to statutes that expressly block or expressly subject information to judicial compulsory process, confidentiality provisions in statutes that are silent on disclosures pursuant to legal process are ambiguous as to their effect on such process.

The SCA falls into this third, ambiguous category. Unlike the many other federal statutes that expressly privilege or exempt information from judicial compulsory process, the word "divulge" in section 2702(a) does not expressly address compelled disclosures pursuant to lawful judicial compulsory process. Hence, it is ambiguous whether Congress intended the SCA's command to "not knowingly divulge" to function like an attorney's ethical and professional duties of confidentiality to a client, which yield to court-ordered subpoenas, or like the attorney-client privilege, which does not.

Importantly, the SCA's legislative history offers no guidance on this matter; it is also silent as to the statute's effect on subpoenas requested by criminal defendants. Nothing in the legislative history indicates that Congress intended the SCA to short-circuit normal judicial compulsory process procedures that serve the truth-seeking and fairness interests of the courts and of society. Nor is there any indication that Congress meant to override the balancing procedures that Oregon's legislature and courts have devised to weigh those interests against overriding needs for secrecy.

B. The Presumption Against Preemption and the *St. Regis* Clear Statement Rule Both Favor Construing the SCA Narrowly to be Consistent with Oregon Law and to Yield to Criminal Defense Subpoenas.

Given the SCA's ambiguous silence as to its effect on judicial compulsory process requested by criminal defendants, two canons of statutory construction

apply. The presumption against federal preemption requires that federal statutes be narrowly construed to avoid preempting state laws except in limited circumstances. Separately, the *St. Regis* clear statement rule requires that federal statutes be strictly construed to avoid suppressing evidence from the truth-seeking process of the courts. Both canons favor narrowly construing the SCA to permit criminal defendants to access evidence that is relevant to their defense using Oregon's well-crafted subpoena rules and the privacy-protective balancing procedures that those rules contain.

i. The Presumption Against Preemption Favors Narrowly Construing the SCA to be Consistent with Oregon Law and Criminal Procedure.

The presumption against federal preemption applies especially strongly in areas like criminal subpoenas that are traditionally regulated by the states: "The court starts with the assumption that the historic police powers of the States were not to be superseded by the Federal Act unless that was the clear and manifest purpose of Congress." *Emerald Steel Fabricators*, 348 Or at 191 (quoting *Wyeth v. Levine*, __ US__, 129 S Ct 1187, 1194-95, 173 L Ed 2d 51 (2009) (cleaned up)). Nonetheless, federal preemption can occur in three circumstances: if it is express, if it is implied by congressional intent to regulate an entire field of conduct exclusively, or if it is implied by an actual conflict between state and federal law. *Id.* at 172. Only the third avenue, conflict preemption, is potentially implicated by the SCA because there is no express preemption language in the SCA and no

indication that Congress meant for this statute to wholly occupy the field. For conflict preemption to apply, it must be "physically impossible to comply with both state and federal law" or state law must "stand[] as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress." *Id.* at 175.

It is not impossible for a private party to comply with both a criminal defense subpoena issued pursuant to ORS 136.580 and the SCA's prohibition on "divulg[ing]" the contents of a communication because submitting information to a court does not 'divulge' anything. A trial court has broad discretion to review the documents *in camera* and fashion appropriate protective measures to maintain privacy. *See Bray*, 363 Or at 252; ORS 135.873(2)-(3). As when trade secret owners, public officials, and DHS submit information to courts for *in camera* review, *in camera* review enables the court to maintain the *secrecy* of the information. And if the court determines that information must be provided to criminal defense counsel, then protective orders, courtroom closures, and sealing orders can ensure continued confidentiality, when appropriate. *Id.*

Nor does compliance with criminal defense subpoenas stand as an obstacle to Congress's purposes in enacting the SCA. "[T]he main goal * * * of the SCA in particular, was to update then existing law in light of dramatic technological changes so as to create a fair balance between the privacy expectations of citizens

and the legitimate needs of law enforcement." *Facebook, Inc. v. Superior Court ("Hunter")* 4 Cal 5th 1245, 1262-63 (2018) (quoting H. R. Rep. No, 99-647, 2d Sess, p 19 (1986)). Accordingly, Congress's purposes in enacting the SCA encompassed "three themes— (1) protecting the privacy expectations of citizens, (2) recognizing the legitimate needs of law enforcement, and (3) encouraging the use and development of new technologies (with privacy protection being the primary focus)." *Id*. at 1263. Congress was particularly concerned that Fourth Amendment protections might not apply to electronic communications stored with third-party service providers and sought to create the SCA to fill that potential gap. *Id*. at 1263 & fn. 15. Nothing in the SCA's text or its legislative history indicates that Congress intended to restrict criminal defense subpoenas.

Enforcing criminal defense subpoenas and *in camera* review procedures to balance defense access rights with countervailing interests in secrecy is not an obstacle to any of these congressional purposes. Compliance with criminal defense subpoenas does not stand in the way of Congress's goal of shoring up Fourth Amendment protections for the electronic age because criminal defense subpoenas co-exist with Fourth Amendment protections. Criminal defense subpoenas reach cell-site location information, papers stored in physical homes, and inspections of private premises without standing as an obstacle to Article I, section 9, and Fourth Amendment protections for those same categories of information or physical

spaces. As but one example, New York State has expressly codified criminal defendants' entitlement to court orders that compel access onto private property, including homes, to enable defendants to inspect "premises relevant to the subject matter of the case." NY Crim Proc Law § 245.30(2). None of these defense-access procedures conflicts with Fourth Amendment protection, and neither do criminal defense subpoenas for stored electronic communications contents. Indeed, this court has already crafted specific protections for digital data obtained pursuant to a defense subpoena that purposefully mirror the same privacy protections required under Article I, section 9. *Bray*, 363 Or at 251-53.

Nor would it undermine citizens' more general privacy expectations to compel Meta to comply with the same subpoena rules that apply to hospitals, banks, telephone service providers, credit card companies, and other businesses that store sensitive information about their users. Far from it, channeling criminal defense subpoenas to Meta would *protect* privacy because Meta has a policy of notifying users when information about them has been subpoenaed. Meta states on its website: "Our policy is to notify people who use our service of requests for their information prior to disclosure[.]" (Information for Law Enforcement Authorities <https://about.meta.com/actions/safety/audiences/law/guidelines> (last accessed Jan. 3, 2025). This notice enables individuals to move to quash a criminal defense subpoena and have the court weigh any privacy interests at stake against the

defendant's need for the information. Although Meta has stated that it failed to provide such notice in this case, that decision was based on its (erroneous) interpretation of the SCA. A holding from this court (correctly) interpreting the SCA to require production for *in camera* review in response to a proper subpoena would thus appear to trigger Meta's notice policy.

As for Congress's goal of recognizing "the legitimate needs of law enforcement," *Hunter*, 4 Cal 5th at 1263, enforcing criminal defense subpoenas serves rather than conflicts with law enforcement needs for truth-seeking, fairness, and justice. Law enforcement has an interest in the integrity of their convictions. This includes avoiding convicting the innocent and avoiding needless reversals on appeal, both of which will result if this court construes the SCA as an absolute bar on criminal defense subpoenas that prevents defense lawyers from being effective and forces them to fail to investigate their clients' cases.

Finally, there is no evidence that enforcing criminal defense subpoenas for information that a court will consider via *in camera* review would discourage people from using Meta's services, which are among the most used social networks in the world. Few people expect to be subject to an investigation *ex ante*. Those who do are more likely to be chilled from using social media by the prospect of law enforcement access than that of a criminal defense attorney. For the vast majority of Meta's 3.35 billion daily active users, such concerns are unlikely to be

salient to their decision to use social media. (Cumulative Number of Daily Meta Product Users <https://www.statista.com/statistics/1092227/facebook-product-dau/> (as of Jan 13, 2025). Enforcing criminal defense subpoenas to hospitals, banks, telephone service providers, credit card companies, and other businesses does not discourage people from using those services, and it will not discourage people from using social media either.

Oregon's well-constructed procedures for balancing criminal defense subpoenas with competing privacy interests do not conflict with either the plain text of the SCA or Congress's goals in enacting it. This Court should apply the presumption against preemption and narrowly construe the SCA to be consistent with Oregon law.

ii. The *St. Regis* Clear Statement Rule Favors Narrowly Construing the SCA to Not Create an Absolute Privilege for the Internet.

The other canon of statutory construction that applies in this case is the *St. Regis* clear statement rule. The United States Supreme Court has instructed courts not to construe a federal statute to block otherwise valid subpoenas unless the plain text of the statue clearly indicates congressional intent to immunize information from legal process. The Court announced this clear statement rule in *St. Regis Paper Company v. United States*, 368 US 208, 218, 82 S Ct 289, 7 L Ed 2d 240 (1961), stating that courts considering 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." "Indeed, when Congress has intended [information] not to be subject to compulsory process it has said so." *Id.* at 218.

Subsequent cases clarified that a federal statute can satisfy the clear statement rule in two circumstances: if it contains express privilege language blocking legal process (*see Pierce County v. Guillen*, 537 US 129, 145, 123 S Ct 720, 154 L Ed 2d 610 (2003)), or by implication if it "embod[ies] explicit congressional intent to preclude *all* disclosure" of covered information, and thus establishes such a "strong policy of nondisclosure [that it] indicates that Congress intended the confidentiality provisions to constitute a 'privilege' within the meaning of the Federal Rules" (*Baldrige v. Shapiro*, 455 U.S. 345, 361, 102 S Ct 1103, 71 L Ed 2d 199 (1982) (emphasis in original)).

The SCA does not contain express privilege language blocking legal process. The Supreme Court has provided at least three examples of federal statutes that do. One stated that covered information "shall [not] be admitted as evidence or used for any purpose in any suit or action for damages." *St. Regis*, 368 US 218 n8). Another stated that "no [covered information] shall be admitted as evidence, or used for any purpose, in any suit or action for damages." *Id.* at 218 n9. The third stated that covered information "shall not be subject to discovery" and "shall not be * * * admitted into evidence." *Pierce County*, 537 US 145. The SCA has no such language. It is totally silent regarding courts' normal powers of

judicial compulsory process. Therefore, the SCA cannot satisfy the *St. Regis* clear statement rule via the express language route.

The SCA also does not imply a privilege by embodying "explicit congressional intent to preclude *all* disclosure" of covered information. *Baldrige*, 455 US at 361. On the contrary, the SCA's confidentiality provision has a plethora of exceptions permitting service providers to divulge stored electronic communications in an array of circumstances, including to addressees, intended recipients, and their agents; with consent from a variety of different possible people; to employees, "authorized" persons, and people whose facilities are used to provide a service; when divulgences are "incident" to protect a service provider's rights or property; and to law enforcement, other governmental entities, and foreign governments under various conditions. *See* 18 USC § 2702(b). Far from establishing such a "strong policy of nondisclosure [that it] indicates that Congress intended the confidentiality provisions to constitute a 'privilege' within the meaning of the Federal Rules," *Baldrige*, 455 US at 361, the SCA's plethora of exceptions establishes a *weak* policy of nondisclosure offering no indication that Congress intended to create an absolute privilege against criminal defense subpoenas.

The United States Supreme Court has provided one example of statutory text that implied a privilege by embodying "explicit congressional intent to preclude *all*

disclosure" of covered information. *Baldrige*, 455 US at 361 (emphasis in original). *Baldrige* concerned "lists of addresses collected and utilized by the Bureau of the Census" that contained "raw census data pertaining to particular individuals." *Id*. at 347, 349. The Court held that two sections of the Census Act, codified at 13 USC § 8(b) and 13 USC § 9(a), prohibited disclosure of the address lists in response to either a Freedom of Information Act or a civil discovery request. *Id*. at 354-56, 360.

The pertinent portion of section 8(b) stated that the Secretary of Commerce must "***not disclose the information*** reported by, or on behalf of, any particular [census] respondent * * *." 13 USC § 8(b), emphasis added (quoted in *Baldrige*, 455 US at 354). The pertinent portions of section 9(a) stated:

> "Information as confidential; exception
>
> "(a) Neither the Secretary, nor any other officer or employee of the Department of Commerce or bureau or agency thereof, or local government census liaison, may, ***except as provided in section 8*** of this title –
>
> "1) ***use the information*** furnished under the provisions of this title for any purpose other than the statistical purposes for which it is supplied; or
>
> "2) ***make any publication*** whereby the data furnished by any particular establishment or individual under this title can be identified * * *

13 USC § 9(a)(1) (emphasis added) (quoted in *Baldrige*, 455 US at 354-55).

That statutory language was nothing like the SCA for at least two reasons. *First,* section 8(b) expressly mandated that the Census Bureau must "not *disclose*" information (13 USC § 8(b), emphasis added), whereas the SCA merely contains an ambiguous prohibition on "divulg[ing]" information (18 USC § 2702(a)). *Second*, unlike the SCA's plethora of exceptions, section 8(b)'s nondisclosure mandate contained no exceptions whatsoever. Meanwhile, the *Baldrige* opinion noted that the pertinent portions of section 9(a) contained only one narrow exception for statistical uses that did not reveal the raw census data. *Baldrige*, 455 US at 356 ("The Secretary is prohibited from using the 'information' except for statistical purposes * * *").[3] Hence, in sharp contrast to the SCA, sections 8(b) and 9(a) of the Census Act really did "preclude *all* disclosure."

The SCA's prohibition on divulgence is thus distinguishable from the Census Act prohibition on disclosure, and the SCA cannot satisfy the *St. Regis* clear statement rule via the implied privilege route from *Baldrige*. This court

[3] Although the *Baldrige* opinion does not mention this, one other exception arguably applied to the section 9(a) prohibitions on use and publication. Section 8(a) permitted the Secretary to furnish a census respondent with "authenticated transcripts or copies of reports (or portions thereof) containing information furnished by, or on behalf of, such respondent * * *." 13 USC § 8(a). Hence, the Secretary could have returned the address list data to the people who provided it in the first place. That additional possible exception was so narrow that it does not undermine the *Baldrige* holding that the Census Act has a "strong policy of nondisclosure," which is readily distinguishable from the plethora of exceptions in the SCA.

should instead construe the SCA narrowly to be consistent with Oregon's normal subpoena procedures.

St. Regis's clear statement rule prevails over the *expressio unius* canon that Meta has advanced in other cases and may advance here. *See, e.g., Roeder v. Islamic Republic of Iran,* 646 F3d 56, 62 (DC Cir 2011) (*expressio unius* is insufficient to overcome a clear statement rule); *Arabian Motors Grp., W.L.L. v. Ford Motor Co*., 775 F App'x 216, 219 (6th Cir 2019) (same). Even if it did not, *expressio unius* cannot resolve the issue in this case. The logic of *expressio unius* is that when Congress knows how to write something and did not, courts should presume the omission was intentional. Here, that logic cuts both ways. Although it is true that Congress knows how to create express exceptions to confidentiality rules and did not create one in the SCA for subpoenas requested by criminal defendants, Congress also knows how to create express privileges barring compulsory process and did not create one in the SCA for subpoenas requested by criminal defendants. *Cf.*, *Hardt v. Reliance Standard Life Ins. Co.*, 560 US 242, 252, 130 S Ct 2149, 176 L Ed 2d 998 (2010) ("Congress knows how to impose express limits on the availability of attorney's fees in ERISA cases. Because Congress failed to include in § 1132(g)(1) an express 'prevailing party' requirement, the Fourth Circuit's decision adding that term of art to the statute more closely resembles 'invent[ing] a statute rather than interpret[ing] one.'").

Therefore, this Court should apply the *St. Regis* clear statement rule to construe the SCA as consistent with the carefully crafted balance in Oregon subpoena law between criminal defendants' interests in accessing relevant evidence and overriding interests in keeping some information secret.

C. Three Federal Circuits Have Narrowly Construed Similar Statutory Text as Consistent with Judicial Compulsory Process.

The United States Courts of Appeal for the Ninth, Tenth, and Eleventh Circuits have all narrowly construed federal confidentiality statutes that are very similar to the SCA as *permitting* disclosures pursuant to court-ordered discovery and to serve truth-seeking interests in criminal proceedings. All three federal circuits considered the following statutory text from the Immigration Reform and Control Act (IRCA), codified at 8 USC § 1255a, or text from the IRCA that is codified at 8 USC § 1160 and is identical in all relevant respects:

> "Confidentiality of Information
>
> "Neither the Attorney General, nor any other official or employee of the Department of Justice, or bureau or agency thereof, may--
>
> "(A) ***use the information*** furnished pursuant to an application filed under this section for any purpose other than to make a determination on the application or for enforcement of paragraph (6) or for the preparation of reports to Congress under section 404 of the Immigration Reform and Control Act of 1986,
>
> "(B) make any ***publication whereby the information*** furnished by any particular individual can be identified, or

> "(C) ***permit anyone*** other than the sworn officers and employees of the Department or bureau or agency or, with respect to applications filed with a designated entity, that designated entity, ***to examine individual applications***; except that the Attorney General may provide, in the Attorney General's discretion, for the furnishing of information furnished under this section in the same manner and circumstances as census information may be disclosed by the Secretary of Commerce under section 8 of Title 13."

8 USC § 1255a(c)(5) (1995) (emphasis added.)

This text is remarkably similar to that of the SCA because both statutes impose broad confidentiality mandates followed by a plethora of enumerated exceptions but silence regarding disclosure pursuant to judicial compulsory process. Regarding confidentiality, the SCA prohibits service providers from 'divulging' communications contents (18 USC § 2702(a)), while the IRCA prohibits the Department of Justice from 'using' or 'publishing' information and from "permit[ting] anyone * * * to examine individual applications" (8 USC § 1255a(c)(5)(A)-(C)). Regarding enumerated exceptions, the SCA expressly authorizes 'divulgences' in a wide array of circumstances, including "to an addressee," to employees, and as "necessarily incident to the rendition of the service[.]" 18 USC § 2702(b). Similarly, the IRCA expressly authorizes 'use' of information in three circumstances: making "a determination on the application," enforcing "penalties for false statements in applications," and preparing "reports to Congress." 8 USC § 1255a(c)(5)(A). It also expressly authorizes 'examination' of applications in three circumstances: by "sworn officers and employees," by a

"designated entity," and in the same manner as "census information" disclosures. 8 USC § 1255a(c)(5)(B). Neither statute contains an express exception for standard judicial compulsory process.

As described in detail below, the Ninth Circuit narrowly construed the IRCA's prohibition on "use" or "publication" of information as not barring court-ordered discovery. The Tenth Circuit narrowly construed the IRCA's prohibition on "use" or "publication" of information as not barring the introduction of information into evidence in a criminal trial. And the Eleventh Circuit narrowly construed the IRCA's prohibition on "permit[ting] anyone * * * to examine individual applications" as not barring court-ordered discovery.

More specifically, the Ninth Circuit construed the IRCA in a class action suit against the Immigration and Naturalization Service (INS), which was an agency of the Department of Justice. In *Zambrano v. I.N.S*, 972 F.2d 1122 (9th Cir. 1992), a federal district court "ordered the INS to provide a list of the names and addresses of [noncitizens who applied for amnesty pursuant to the IRCA] to the court and the class counsel." *Id.* at 1124. In other words, this was a court order to disclose "information furnished pursuant to an application" that would identify "particular individual[s]," so it potentially conflicted with the IRCA's prohibitions on "use" and "publication." Accordingly, the INS argued that the IRCA acted "as a complete bar to the disclosure of the names to the district court and class counsel."

Id. at 1125. Instead, the Ninth Circuit held that the IRCA's "confidentiality provision is not violated by [] court ordered discovery" because it "does not specifically prohibit judicial disclosure." *Id.* at 1125-26. The Ninth Circuit reasoned that "statutes prohibiting general disclosure of information do not bar judicial discovery absent an express prohibition against such disclosure." *Id.* at 1125 (citations omitted). Applying the same reasoning to the SCA would mean that the SCA's prohibition on 'divulging' communications contents does not bar judicial discovery because it does not expressly prohibit such disclosure.

The Tenth Circuit construed the IRCA in a criminal case in *United States v. Hernandez*, 913 F.2d 1506 (10th Cir 1990). Zenon Hernandez was convicted by a jury of making false statements in connection with the acquisition of a firearm and receiving a firearm while illegally in the United States. *Id.* at 1509. To prove that Hernandez was in the country illegally, the government introduced into evidence a "computer printout from the INS indicat[ing] that Hernandez applied for amnesty to legalize his immigration status[.]" *Id*. The printout revealed individually-identifying information that Hernandez had "provided in the context of [his] application," *id.* at 1511, so it potentially conflicted with the IRCA's prohibitions on "use" and "publication." On appeal, Hernandez argued that the IRCA prohibited the government from introducing this evidence. *Id.* at 1510. The Tenth Circuit acknowledged that "[o]ne reading of the statute would suggest that *any* disclosure

of information is prohibited," but reasoned that the statutory language was "somewhat ambiguous as to the scope of the confidentiality requirement." *Id.* at 1511. Given this ambiguity, the Tenth Circuit consulted the legislative history of the statute and found that the "legislative history does not indicate that Congress sought to restrict disclosure of such applications" in run-of-the-mill criminal proceedings. *Id.* at 1512. As a result, the Tenth Circuit held that the IRCA did not bar introducing the printout as evidence in court. *Id*.

Applying the same reasoning to the SCA would mean that, since the SCA's prohibition on 'divulging' is also ambiguous as to scope, and since the SCA's legislative history never indicates that Congress intended to restrict standard judicial compulsory process, the SCA does not bar subpoenas requested by criminal defendants.

The Eleventh Circuit construed the IRCA in another class action suit against the INS. In *In re Nelson*, 873 F.2d 1396 (11th Cir 1989), a federal district court ordered the INS to grant plaintiffs "access to files of applicants for Special Agricultural Worker ("SAW") status." *Id.* at 1397. In other words, this was a court order to disclose application files, so it potentially conflicted with the IRCA's prohibition on "permit[ting] anyone * * * to examine individual applications." The INS argued that "the district court's order violates the confidentiality requirement embodied in [the IRCA], which prohibits Justice Department officials from

disclosing information from files of SAW applicants." *Id.* The Eleventh Circuit responded to the statute's textual ambiguity by consulting its legislative history and concluded that: "There is no indication that Congress intended to prohibit disclosure of SAW application files in judicial proceedings * * *. The district court's protective order restricting use of the information for purposes of discovery and trial preparation adequately ensures that disclosure will be limited to counsel and their assistants." *Id*. Hence, the Eleventh Circuit held that the IRCA's prohibition on "permit[ting] anyone * * * to examine individual applications" does not bar court-ordered discovery of individual applications. *Id*. Applying the same reasoning to the SCA would mean that the SCA's prohibition on "divulging" communications contents does not bar court-ordered discovery of communications contents.

Meta's attempt to distinguish these persuasive precedents from three different United States Courts of Appeal in a pending case similar to this one (*Snap Inc., Meta Platforms, Inc. v. Superior Court of San Diego County*, Supreme Court of California Case No. S286267) should not convince this court to adopt its interpretation. *Amici* address Meta's arguments in that case here in an abundance of caution, should Meta reprise the same arguments before this court.

To start, Meta inexplicably ignored that the IRCA prohibited the Department of Justice from "permit[ting] anyone * * * *to examine* individual applications," and

erroneously contended that the text "precluded only the '*use*' or '*publication*' of immigration information." This is not true. In addition to prohibiting the "use" and "publication" of information, the IRCA's text also prohibits the "examination" of applications.

Meta's omission is particularly strange for three reasons. *First*, the Tenth Circuit made it hard to miss the "to examine" statutory language by quoting that language in the main text of its opinion. *See Hernandez*, 913 F2d at 1511. *Second*, the Eleventh Circuit's holding applied directly to the "to examine" language because the court ruled that the IRCA does not bar court-ordered discovery of "SAW *application files*." *In re Nelson*, 873 F2d at 1397 (emphasis added). *Third*, the Tenth Circuit's opinion also implicated the "to examine" language because, while the computer printout at issue in that case was not a full application file, the court's reasoning addressed applications, not merely information. *See Hernandez*, 913 F2d at 1512 ("[Congress's] concern is not implicated when the *application* is disclosed to a United States Attorney in a collateral criminal prosecution * * *." (emphasis added)).

Meta relied on its curious omission of the "to examine" language to argue that the Ninth, Tenth, and Eleventh Circuit cases "say nothing about statutory language, like the SCA's, that prohibits the *disclosure* of information—because one could disclose information in response to a subpoena without 'using' or

'publishing' it." But the SCA's statutory language does not prohibit the *disclosure* of information; on the contrary, it mandates that service providers "shall not knowingly *divulge*" information. 18 USC § 2702(a), emphasis added). It is ambiguous whether the word "divulge" in the SCA includes limited and controlled disclosures pursuant to judicial compulsory process.

The Ninth, Tenth, and Eleventh Circuit cases should inform this Court's analysis of the SCA because they show that broad statutory confidentiality provisions can be ambiguous as to their effect on disclosures pursuant to judicial compulsory process. The Ninth Circuit narrowly construed a statutory prohibition on "use" and "publication" as "not violated by [] court ordered discovery." *Zambrano*, 972 F2d at 1125. The Tenth Circuit narrowly construed a statutory prohibition on "use" and "publication" as not violated by introducing information into evidence at trial. *Hernandez*, 913 F2d at 1512. And the Eleventh Circuit narrowly construed a statutory prohibition on "permit[ting] anyone * * * to examine individual applications" as not violated by court-ordered discovery. *In re Nelson*, 873 F2d at 1397. The principles and reasoning unifying these three courts' holdings suggest that—to paraphrase Meta—one could also disclose information in response to a subpoena without "divulg[ing]" it.

Rather than admit the logic of the Ninth, Tenth, and Eleventh Circuits, Meta pointed to a case from the D.C. Circuit, *In re England*, 375 F.3d 1169 (DC Cir

2004). But the statutory language at issue in *In re England* was distinguishable from the SCA. At the time, the statute in that case stated that board deliberations concerning military personnel promotions "may not be disclosed to any person not a member of the board." 10 USC § 618(f) (2000). It never used the ambiguous term "divulge" that appears in the SCA. Further, the disclosure bar at issue in *In re England* had merely a narrow set of exceptions allowing the board to send reports up the chain of command to the President, exceptions which are necessary to effectuate the purpose of the statute as a whole. *See* 10 USC § 618(a)-(c), (e) (2000)). The narrowness of those exceptions makes the statute similar to the one at issue in *Baldrige*, "embody[ing] explicit congressional intent to preclude *all* disclosure," 455 US at 361, and nothing like the plethora of exceptions to the SCA's confidentiality provision.

In sum, the statutory language at issue in *Zambrano*, *Hernandez*, and *Nelson* was remarkably similar to the text of the SCA, and United States Courts of Appeal for the Ninth, Tenth, and Eleventh Circuits all agreed that it did not preclude limited and controlled disclosures pursuant to lawful judicial compulsory process. *See also* Jack B. Weinstein & Margaret A. Berger, *Weinstein's Federal Evidence* § 502A.05(I) (2d ed) ("[S]tatutes asserted to create privileges should be construed strictly, so as to avoid suppressing otherwise competent evidence unless *no other conclusion* can be drawn from the statutory language." (emphasis added). This

court should apply similar reasoning to the SCA and conclude that the SCA is consistent with Oregon law's careful balancing of criminal defendants' need to have access to relevant evidence to prepare their defense and the simultaneous need to protect overriding interests in secrecy.

D. Numerous Federal District Courts Have Narrowly Construed Similar Statutory Text as Consistent with Judicial Compulsory Process.

Federal district courts across the country have applied similar reasoning to the Ninth, Tenth, and Eleventh Circuits and narrowly construed confidentiality mandates in an array of other federal statutes as not barring compliance with normal judicial compulsory process. These cases show that even statutory language prohibiting "disclosure" can be ambiguous as to its effect on judicial compulsory process, and that numerous courts have construed such ambiguous language narrowly to be consistent with the truth-seeking procedures of the courts. *See, e.g., In re Nassau Cnty. Strip Search Cases*, No. 99-cv-2844, WL 3189870 at *2 & *6 (EDNY July 26, 2017) (statutory prohibitions on "the use or disclosure of information" did not block court-ordered discovery because the text never "specifically provides that information is not subject to discovery"); *Rodriguez v. Robbins*, No. 07-cv-3239, WL 12953870 at *2-*3 (CD Cal May 3, 2012) (statutory prohibitions on "permit[ting] use by or disclosure to anyone" did not block legal process because "statutory provisions, generally forbidding disclosure of information, do not bar judicial discovery absent an explicit prohibition against

such disclosure"); *Hassan v. United States*, No. C05-1066C, WL 681038, at *2-*3 (WD Wash Mar 15, 2006) (statutory requirement to "limit the use or disclosure of information" did not block legal process because "statutes prohibiting general disclosure of information do not bar judicial discovery absent an express prohibition against such disclosure"); *Chaplaincy of Full Gospel Churches v. England*, 234 FRD 7, 12 (DDC 2006) (statute stating that protected information "may not be disclosed to any person" did not block legal process because of "the well established requirement that statutory bars to discovery be made expressly"); *Seales v. Macomb Cnty.* 226 FRD 572, 575-76 (ED Mich 2005) (statute designating information "confidential," safeguarding "disclosure of this information," and mandating that it "not be made public," did not block legal process because "[s]tatutory provisions providing for duties of confidentiality do not automatically imply the creation of evidentiary privileges binding on courts."); *Wilkins v. United States*, No. 99-cv-1579, US Dist LEXIS 29428 at *16-*17 (SD Cal Dec 23, 2004) (observing that courts must "avoid construing a confidentiality provision in a statute as barring disclosure for discovery purposes unless the statute clearly requires such suppression"); *In re Grand Jury Subpoena Duces Tecum*, No. 101-mc-00005, WL 896479, at *3-*4 (WD Va June 12, 2001) (construing a statutory requirement to "limit the use or disclosure of information," the court reasoned that, "based on my duty to strictly construe statutes purporting to create

new privileges, I find that the statutes and regulations at issue here do not create a statutory privilege[.]").

In sum, even statutory prohibitions on "disclosure" do not always unambiguously bar compliance with judicial compulsory process. The SCA's vague prohibition on "divulg[ence]" is more ambiguous still.

IV. Misconstruing the SCA as Blocking all Subpoenas Would Create an Outlier Privilege for a *Medium* of Communication, Without Regard to the Relationship Between the Communicants or the Sensitivity of their Communications.

Misconstruing the SCA to block so-ordered criminal defense subpoenas, rather than merely to protect confidentiality in circumstances other than court-ordered *in camera* review, would create a vast and unprecedented privilege immunizing an entire *medium* of communication from the court's truth-seeking process, without regard to the communicants' purpose, topic, or expectations of confidentiality. The result would undermine judicial truth-seeking with no clear societal benefit.

Barring exceptional topical privileges like military and trade secrets, privileges protect narrow categories of communications arising out of specific relationships. The attorney-client privilege and spousal privilege apply solely to communications between a lawyer and a client or between spouses respectively, and solely to communications made in confidence in reliance on that relationship. *See* OEC 503; OEC 505. The statutory privilege in *Baldrige* also protected a

specific relationship between citizens and the Census Bureau for the purpose of facilitating census reporting. 455 US at 354.

But the SCA is neither topic nor relationship specific. There is no indication in the SCA's text or legislative history that Congress intended it to create a novel "medium privilege" for any and all communications that happen to be sent over the Internet. If service providers want a special exemption from the burdens of complying with judicial process that other business, private persons, and even Presidents must bear (*cf. Trump* v. *Vance*, 591 US 786, 810, 140 S Ct 2412, 207 L Ed 2d 907 (2020) ("[N]o citizen, not even the President, is categorically above the common duty to produce evidence when called upon in a criminal proceeding.")), then the service providers can ask Congress to grant them such a privilege via unambiguous statutory text. In the meantime, this court should not construe ambiguous silence in the SCA to gift such special treatment to technology markets.

CONCLUSION

For the foregoing reasons, we urge the Court to require the trial court to enforce Mr. Ayon-Urbano's subpoena by holding that 18 USC § 2702(a) is consistent with Oregon law governing judicial compulsory process requested by criminal defendants and does not preempt the *camera* review procedure that Mr. Ayon-Urbano requested here.

DATED January 13, 2026.

Respectfully Submitted,

DEAN ERWIN CHEMERINSKY
UC Berkeley School of Law

PROFESSOR REBECCA WEXLER
Columbia Law School

CHESA BOUDIN
Executive Director, Criminal Law & Justice Center
UC Berkeley School of Law

s/ Lindsey Burrows
_____
Lindsey Burrows
OSB No. 113431
333 SW Taylor St, Suite 300
Portland, OR 97204
(503) 882-4575
lindsey@burrowsappellatelaw.com
Of Attorneys for *Amici Curiae*