

No. 26-208

IN THE
Supreme Court of the United States

GEORGE ANIBOWEI,
Petitioner,

v.

TODD BLANCHE, U.S. ATTORNEY GENERAL,
ET AL.,
Respondents.

**On Petition for Writ of Certiorari to the
United States Court of Appeals for the
Fifth Circuit**

**BRIEF OF AMICUS CURIAE AMERICAN BAR
ASSOCIATION IN SUPPORT OF PETITIONER**

JO-ANN TAMILA SAGAR
MICHAEL J. WEST
JACKSON B. SKEEN
HOGAN LOVELLS
CADWALADER US LLP
555 Thirteenth St., N.W.
Washington, D.C. 20004

BARBARA J. HOWARD
Counsel of Record
PRESIDENT
AMERICAN BAR ASSOCIATION
321 N. Clark St.
Chicago, IL 60654
312-988-5000
amicusbriefs@americanbar.org

ERICA J. SHULER
HOGAN LOVELLS
CADWALADER US LLP
8350 Broad St., Floor 17
Tysons, VA 22102

Counsel for Amicus Curiae American Bar Association

TABLE OF CONTENTS

	<u>Page</u>
TABLE OF AUTHORITIES.....	ii
STATEMENT OF INTEREST	1
INTRODUCTION AND SUMMARY OF ARGUMENT	4
ARGUMENT	7
I. THE QUESTION PRESENTED IMPLICATES SUBSTANTIAL PRIVACY AND CONFIDENTIALITY INTERESTS.....	7
II. ATTORNEYS HAVE HEIGHTENED PRIVACY AND CONFIDENTIALITY INTERESTS IN THE CONTENTS OF THEIR ELECTRONIC DEVICES	8
A. Attorneys Have A Duty To Maintain Confidentiality Over Client Information On Their Devices.....	12
B. Attorneys Are Under An Obligation To Preserve Privileged Communications On Their Devices	14
C. Absent Judicial Supervision, Border Searches Of Attorneys' Devices Impose Unique Burdens On Attorneys And Their Clients.....	16
III. THIS COURT SHOULD RESOLVE THE QUESTION PRESENTED TO PROVIDE NEEDED CLARITY FOR ATTORNEYS AND THEIR CLIENTS	19
CONCLUSION	22

TABLE OF AUTHORITIES

	<u>Page(s)</u>
CASES:	
<i>Carpenter v. United States</i> , 585 U.S. 296 (2018).....	8
<i>Chatrie v. United States</i> , 146 S. Ct. 2193 (2026).....	2, 4, 7, 8
<i>Commodity Futures Trading Comm’n v. Weintraub</i> , 471 U.S. 343 (1985).....	15
<i>DR Distribs., LLC v. 21 Century Smoking, Inc.</i> , 513 F. Supp. 3d 839 (N.D. Ill. 2021).....	14
<i>Fisher v. United States</i> , 425 U.S. 391 (1976).....	14
<i>Hiscox Ins. Co. v. Warden Grier, LLP</i> , 474 F. Supp. 3d 1004 (W.D. Mo. 2020).....	14
<i>Hunt v. Blackburn</i> , 128 U.S. 464 (1888).....	15
<i>In re Conduct of Conry</i> , 491 P.3d 42 (Ore. 2021)	13
<i>Jaffee v. Redmond</i> , 518 U.S. 1 (1996).....	15
<i>James v. Nat’l Fin. LLC</i> , No. 8931-VCL, 2014 WL 6845560 (Del. Ch. Dec. 5, 2014)	14
<i>Mohawk Indus., Inc. v. Carpenter</i> , 558 U.S. 100 (2009).....	15
<i>People v. Braham</i> , 470 P.3d 1031 (Colo. 2017)	13

TABLE OF AUTHORITIES—Continued

	<u>Page(s)</u>
<i>Riley v. California</i> , 573 U.S. 373 (2014).....	4, 7-9, 11, 21
<i>Swidler & Berlin v. United States</i> , 524 U.S. 399 (1998).....	15
<i>United States v. Wise</i> , 74 F.4th 953 (8th Cir. 2023)	17
<i>Upjohn Co. v. United States</i> , 449 U.S. 383 (1981).....	15
 RULES:	
Sup. Ct. R. 37.2.....	1
Sup. Ct. R. 37.6.....	1
Model Rules of Pro. Conduct r. 1.1 (ABA 1983)	13
Model Rules of Pro. Conduct r. 1.1 cmt. 8 (ABA 2012)	13
Model Rules of Pro. Conduct r. 1.4(a)(1) (ABA 1983)	18
Model Rules of Pro. Conduct r. 1.4(a)(3) (ABA 1983)	18
Model Rules of Pro. Conduct r. 1.4(a)(4) (ABA 1983)	18
Model Rules of Pro. Conduct r. 1.6(a) (ABA 1983)	12
Model Rules of Pro. Conduct r. 1.6(c) (ABA 1983)	13, 18
Model Rules of Pro. Conduct r. 1.6 cmt. 2 (ABA 2002)	12
Model Rules of Pro. Conduct r. 1.6 cmt. 3 (ABA 1983)	13

TABLE OF AUTHORITIES—Continued

	<u>Page(s)</u>
OTHER AUTHORITIES:	
ABA Resolution 05A111 (Aug. 9, 2005), https://www.americanbar.org/content/dam/aba/directories/policy/annual-2005/2005-am-111.pdf	3
ABA Resolution 19M107A (Jan. 28, 2019), http://www.americanbar.org/content/dam/aba/directories/policy/midyear-2019/107a-midyear-2019.pdf	3, 5, 7, 18-20
Am. Bar Ass’n, <i>Model Rules of Professional Conduct</i> , https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct	3
<i>Attorneys’ Duties to Protect Client Data</i> , Practical Law Practice Note w-014-0379, State Survey: Adopted Duty to Prevent Inadvertent or Unauthorized Disclosure Rule.....	12
W. Bishop, Pew Research Center, Mobile Fact Sheet (Nov. 20, 2025).....	7
CBP Directive No. 3340-049A, Border Search of Electronic Devices (Jan. 4, 2018)	20, 21
Hon. Daniel J. Crothers & Barbara S. Gillers, <i>Electronic Device Advisory for Mid-Year Meeting Attendees</i> , ABA (Jan. 10, 2018), https://perma.cc/2SQN-CMYA	16, 17, 19

TABLE OF AUTHORITIES—Continued

	<u>Page(s)</u>
Clio, <i>2022 Legal Trends Report</i> , https://www.clio.com/wp-content/uploads/2022/09/2022-Legal-Trends-Report-16-02-23.pdf	9
Philip George, <i>Considerations for Communicating with Clients via Text Message</i> , ABA Litig. Section, Ethics & Professionalism Comm. (Jan. 27, 2023), https://perma.cc/KR7A-746M	9
Robert Hartigan, <i>2024 Budgeting and Planning TechReport</i> , ABA Law Prac. Div., Legal Tech. Res. Ctr. (Apr. 22, 2025), https://perma.cc/2LNM-K9TX	10
Letter from Linda Klein, President, ABA, to Gen. John F. Kelly, Sec’y of Homeland Sec., U.S. Dep’t of Homeland Sec. (May 5, 2017), https://perma.cc/2C9P-DN5X	9, 20
A. Nayak, <i>The Mobile-AI Gap: The Problem in Legal Tech No One is Talking About</i> , Artificial Law. (Mar. 3, 2026), https://perma.cc/R3GJ-VBZB	8, 9
N.Y.C. Bar Ass’n Comm. on Pro. Ethics, Formal Op. 2017-5 (2017)	9
Anna Stolley Persky, <i>As Customs and Border Protection Agents Search More Electronic Devices, How Can Lawyers Keep Client Information Secure?</i> , 112 ABA, Winter 2026	17, 18

TABLE OF AUTHORITIES—Continued

	<u>Page(s)</u>
Steven M. Puiszis, <i>Can't Live with Them, Can't Live without Them—Ethical and Risk Management Issues for Law Firms that Adopt a “BYOD” Approach to Mobile Technology</i> , 2015 J. Prof. Law. 33 (2015).....	11
Restatement (Third) of the Law Governing Lawyers § 68 (2000)	14
Jeff Richardson, <i>2022 ABA Tech Survey provides information on attorney use of iPhones and iPads</i> , iPhone J.D. (Nov. 28, 2022), https://perma.cc/5ZKF-K4JK	10
Mariah L. Sukalski, <i>Lawyers Have Duty to Protect Client Contacts in Smartphones</i> , 49 Litig. News, Fall 2023.....	10
<i>The New Wigmore: Evidentiary Privileges</i> § 3.2.3 (4th ed. 2022).....	15
E. Norman Veasey, <i>Protection of Client Confidential Information from Cyberattacks Is a Compelling Business and Ethical Priority for inside and outside Corporate Counsel</i> , 75 Bus. Law. 1495 (Winter 2019-2020)	17

IN THE
Supreme Court of the United States

GEORGE ANIBOWEI,
Petitioner,

v.

TODD BLANCHE, U.S. ATTORNEY GENERAL,
ET AL.,
Respondents.

**On Petition for Writ of Certiorari to the
United States Court of Appeals for the
Fifth Circuit**

STATEMENT OF INTEREST¹

The American Bar Association (ABA) is the world's largest voluntary association of attorneys and legal professionals. Its membership spans all fifty States, the District of Columbia, and the United States territories, and includes attorneys, legislators, law professors, students, and others.² Many members must travel internationally for work because, for example, they practice for international law firms, represent

¹ Counsel of record for the parties received timely notice of *amicus*'s intent to file this brief. See Sup. Ct. R. 37.2. No party or counsel for a party authored this brief in whole or in part. No party, counsel for a party, or person other than *amicus* or its counsel made any monetary contribution intended to fund the preparation or submission of this brief. See Sup. Ct. R. 37.6.

² The ABA's membership includes judges. However, neither this brief nor the decision to file it reflects the views of any judicial members of the ABA. The Judicial Division Council did not participate in the adoption or endorsement of this brief and did not receive a copy of this brief before filing.

international clients, and work on cases with international aspects.

The ABA’s mission is to advocate for the rights of its members and the interests of the legal profession more broadly. It does this by working to promote ethical conduct among members of the profession, and by advocating for increased public respect for the justice system and attorneys’ roles in it. ABA members look to the organization for guidance in navigating changes to the legal practice, including technological changes that require additional guideposts to safeguard attorneys’ and their clients’ information. The ABA regularly files *amicus* briefs in cases implicating the rights and responsibilities of its member attorneys.³

Attorneys, like the Petitioner in this case, routinely carry electronic devices containing confidential client information and privileged communications, as well as everyday personal information. For this reason, government searches of an attorney’s electronic devices (just like his briefcase) threaten every attorney’s ethical obligations to safeguard client information and preserve the attorney-client privilege, as well as their own personal privacy interests. *See, e.g., Chatrue v. United States*, 146 S. Ct. 2193, 2199-2200 (2026).

The ABA is well positioned to bring this Court’s attention to the heightened privacy and privilege concerns presented by such searches. The ABA has long advocated for the protection of such interests. For

³ *See, e.g.,* ABA Amicus Br. 3, *In re Grand Jury*, No. 21-1397 (U.S. Nov. 23, 2022) (describing the importance of the attorney-client privilege in “the fair operation of our adversarial system of justice”); ABA Amicus Br. 2-3, *Supreme Ct. of N.M. v. United States*, No. 16-1323 (U.S. June 5, 2017) (supporting the application of state rules of professional conduct to federal prosecutors).

example, in 2005, the ABA adopted Resolution 05A111, which affirms the ABA's opposition to "policies, practices, and procedures of governmental bodies that have the effect of eroding the attorney-client privilege and work product doctrine."⁴ Similarly, in 2019, the ABA adopted Resolution 19M107A, which "urges the federal judiciary to recognize the substantial privacy and confidentiality interests, as well as the important national security and law enforcement interests, implicated by searches and seizures of electronic devices at the border."⁵ That Resolution also expresses support for measures to "fully protect the attorney-client privilege, the work product doctrine, and the lawyer's ethical obligation to maintain confidential information during border crossings."⁶

The ABA also has substantial expertise regarding the ethical obligations implicated by border searches of attorneys' devices. Through the Model Rules of Professional Conduct, which "serve as models for the ethics rules of most jurisdictions,"⁷ and related ethics guidance in Formal Ethics Opinions, the ABA has helped define lawyers' duties to preserve confidential client information and address technological risks

⁴ ABA Resolution 05A111 at 1 (Aug. 9, 2005), <https://www.americanbar.org/content/dam/aba/directories/policy/annual-2005/2005-am-111.pdf>.

⁵ ABA Resolution 19M107A (Jan. 28, 2019), <http://www.americanbar.org/content/dam/aba/directories/policy/midyear-2019/107a-midyear-2019.pdf>.

⁶ *Id.*

⁷ See Am. Bar Ass'n, *Model Rules of Professional Conduct*, https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct.

associated with protecting it. The question presented directly implicates those duties and risks.

The ABA’s longstanding positions, advocacy, and expertise in the issues implicated by the border-search exception, as well as the harms the current state of the law works on the ABA’s attorney members, give the ABA and its members a strong interest in the resolution of this case.

INTRODUCTION AND SUMMARY OF ARGUMENT

Modern electronic devices occupy a unique place in the lives of attorneys and their clients, as they do with nearly all Americans. *See Chatrie*, 146 S. Ct. at 2200. Smartphones and laptops are no longer mere communication tools; they are repositories of immense quantities of personal and professional information, including confidential and privileged client communications, attorney work product, and litigation strategies. This Court has repeatedly recognized that electronic devices, while similar to private physical containers, differ significantly due to both the huge volume of information they contain and the intimate portrait they can provide of a person’s life. *E.g.*, *Riley v. California*, 573 U.S. 373, 393-397 (2014); *Chatrie*, 146 S. Ct. at 2205-09. Yet the circuits are divided over how the border-search exception to the Fourth Amendment applies to cell phones. In light of the “substantial privacy and confidentiality interests” raised by searches of electronic devices at the border—in particular searches of devices owned by attorneys like Petitioner—and the need to “fully protect the attorney-client privilege, the work product doctrine, and the lawyer’s ethical obligation to maintain confidential

information during border crossings,”⁸ the ABA urges this Court to grant the petition.

Modern cell phones are ubiquitous and contain vast quantities of sensitive information. This Court has recognized that smartphones have become a universal feature of modern life and can contain immense quantities of personal information. Because electronic devices may contain years of emails, messages, location information, photographs, documents, and other personal records, searches of those devices implicate privacy interests far greater than those associated with traditional searches.

This is especially true as to electronic devices possessed and used by attorneys. Attorneys increasingly rely on smartphones, laptops, and other portable electronic devices to communicate with clients, store work product, and manage active matters. The widespread adoption of mobile technology and workplace policies permitting attorneys to use their own devices for work means that attorneys frequently carry both personal information and client-related materials on a single device.

Attorneys (like Petitioner) have heightened privacy interests in their devices in light of their ethical duty of confidentiality and the attorney-client privilege. ABA Model Rule 1.6 broadly protects all information relating to client representation and requires attorneys to take reasonable steps to prevent inadvertent and unauthorized disclosure or unauthorized access to such information. This duty extends beyond attorney-client privileged communications and encompasses information from any source relating to the

⁸ Resolution 19M107A, *supra*.

representation. The attorney-client privilege, in turn—which is among the oldest and most fundamental protections recognized in American law—protects confidential communications between an attorney and her client for the purpose of providing or obtaining legal assistance. The privilege, like the duty of confidentiality, promotes full and candid communication between attorneys and clients, thereby enabling effective legal representation and advancing the administration of justice.

Warrantless border searches of attorneys’ electronic devices threaten attorneys’ important ethical duty of confidentiality and the attorney-client privilege. A warrantless search of even one attorney’s device could expose significant amounts of confidential and privileged information to third parties. In light of those concerns, the ABA has identified measures legal professionals can take to navigate their ethical obligations under the border-search exception, such as by traveling with an inexpensive phone scrubbed of any confidential information. Such steps are highly unusual, costly, and burdensome, both to the attorney’s ability to remain in contact with clients and to practice while traveling. Moreover, the split among the circuits over the question presented means that an attorney’s obligations differ depending on the jurisdiction from which they enter the United States.

For all the foregoing reasons, and to provide national clarity, this Court should grant certiorari. The ABA has long urged the “federal judiciary to recognize the substantial privacy and confidentiality interests, as well as the important national security and law enforcement interests, implicated by searches and

seizures of electronic devices at the border.”⁹ Petitioner’s work phone—which contained sensitive client information—was searched without a warrant over his vigorous protests. As a result, he no longer travels with his work phone, to the detriment of his clients and his own interests.

ARGUMENT

I. THE QUESTION PRESENTED IMPLICATES SUBSTANTIAL PRIVACY AND CONFIDENTIALITY INTERESTS.

Without judicial supervision, the border-search exception to the Fourth Amendment exposes the entirety of a traveler’s electronic data to government agents.

Smartphones have long been ubiquitous. For over a decade, cell phones have been a “pervasive and insistent part of daily life.” *Riley*, 573 U.S. at 385. Today, reports show that about 91% of Americans own a smartphone, while approximately 98% own a cell phone of some kind. *See Chatrrie*, 146 S. Ct. at 2200 (citing W. Bishop, Pew Research Center, Mobile Fact Sheet (Nov. 20, 2025)).

Just as cell phone use has surged over the past quarter century, so too has the amount of information that cell phones can store. This Court has likened the modern smartphone to a “minicomputer[] that also happens to have the capacity to be used as a telephone,” and has emphasized that cell phones differ from traditional physical objects in both a “quantitative and a qualitative sense.” *Riley*, 573 U.S. at 393. Even a “basic” phone may contain “photographs, picture

⁹ Resolution 19M107A, *supra*.

messages, text messages, Internet browsing history, a calendar, a thousand-entry phone book, and so on,” while modern smartphones can store “millions of pages of text, thousands of pictures, or hundreds of videos.” *Id.* at 393-394. The devices now carried by an overwhelming majority of Americans thus contain vast quantities of sensitive information that can “reveal much more in combination than any isolated record.” *Id.* at 394.

Cell phones also generate a continuous stream of data reflecting their users’ activities, communications, and locations at specific points in time. They produce records that are “detailed, encyclopedic, and effortlessly compiled,” including “time-stamped record[s]” of a user’s location, *Carpenter v. United States*, 585 U.S. 296, 301, 309 (2018), as well as detailed information about the user collected by “apps and other services,” *Chatrie*, 146 S. Ct. at 2200 (quoting *Riley*, 573 U.S. at 396).

II. ATTORNEYS HAVE HEIGHTENED PRIVACY AND CONFIDENTIALITY INTERESTS IN THE CONTENTS OF THEIR ELECTRONIC DEVICES.

Attorneys are not immune to this technological and societal sea-change. Modern smartphones have become as “indispensable” to the practice of law as they are “to participation in modern society.” *Carpenter*, 585 U.S. at 315. Like the general public, attorneys routinely carry their phones at all hours of the day, seven days a week.¹⁰ They do so to stay informed on

¹⁰ A. Nayak, *The Mobile-AI Gap: The Problem in Legal Tech No One is Talking About*, Artificial Law. (Mar. 3, 2026),

their matters, connected to their practice, and in touch with their clients. Attorneys’ constant availability is, in part, a product of their clients’ expectations: “[C]lients increasingly expect their lawyers to be responsive at all hours—including via text message.”¹¹

In addition to the “millions of pages of text, thousands of pictures, or hundreds of videos” housed on any particular phone, *Riley*, 573 U.S. at 393, attorneys’ devices contain confidential and privileged information. For example, a device may contain emails, texts, or other communications across internet-based messaging apps relating to the representation of a client. A device may also contain drafts of briefs, sealed material, notes about a client’s litigation strategy, or scheduled meetings concerning litigation that has not commenced or transactions that have not been announced.¹² Even something as innocuous as a contact

<https://perma.cc/R3GJ-VBZB> (from a 2026 study of 200 legal professionals, reporting that 89% of respondents “check work messages multiple times outside standard hours”); *see also* Clio, 2022 *Legal Trends Report* at 36, <https://www.clio.com/wp-content/uploads/2022/09/2022-Legal-Trends-Report-16-02-23.pdf> (reporting that “86% of lawyers work outside of the typical work day * * * and 73% work outside of regular business days”) (free registration required to access report).

¹¹ Philip George, *Considerations for Communicating with Clients via Text Message*, ABA Litig. Section, Ethics & Professionalism Comm. (Jan. 27, 2023), <https://perma.cc/KR7A-746M>.

¹² *See* Letter from Linda Klein at 1, President, ABA, to Gen. John F. Kelly, Sec’y of Homeland Sec., U.S. Dep’t of Homeland Sec. (May 5, 2017), <https://perma.cc/2C9P-DN5X> (lawyers’ electronic devices “typically contain information that is inherently privileged or otherwise confidential”); N.Y.C. Bar Ass’n Comm. on Pro. Ethics, Formal Op. 2017-5 at 2 (2017) (searches of attorneys’ electronic devices at the border may involve the “review of

page may contain “identifying information about the person the contact represents.”¹³

Put simply, what once resided in filing cabinets, correspondence files, banker boxes, legal pads, and briefcases is now frequently consolidated onto a single device.

Complicating matters further, in recent years, attorneys’ personal cell phone use has surged with the advent of “Bring-your-own-device” (BYOD) policies, which permit employees to use the same device for both personal and business purposes. According to the ABA’s 2024 Legal Technology Survey, one third of respondents said their firm has a BYOD policy in place; and in 2022, almost every respondent reported they can use their personal devices to access their firm’s network.¹⁴ Adopting a BYOD approach improves efficiency, not least because it allows for the consolidation of devices and provides attorneys with the flexibility to work using their preferred devices.

information stored on them, such as emails, text messages and electronically-stored documents”).

¹³ See Mariah L. Sukalski, *Lawyers Have Duty to Protect Client Contacts in Smartphones*, 49 Litig. News, Fall 2023, at 7 (noting that a contact page may contain confidential information such as the contact’s “phone numbers, email addresses, work or residence addresses, employer, birthday, nicknames, and a notes section that could contain further information about the individual or how the phone owner knows the person”).

¹⁴ Robert Hartigan, *2024 Budgeting and Planning TechReport*, ABA Law Prac. Div., Legal Tech. Res. Ctr. (Apr. 22, 2025), <https://perma.cc/2LNM-K9TX>; see also Jeff Richardson, *2022 ABA Tech Survey provides information on attorney use of iPhones and iPads*, iPhone J.D. (Nov. 28, 2022), <https://perma.cc/5ZKF-K4JK>.

Attorneys, however, do not and cannot sacrifice their ethical obligations for the sake of convenience. Indeed, commingling personal and work devices “triggers a number of unique risks for lawyers and law firms”; primarily, the risk that non-public information may be disclosed.¹⁵ As a result, lawyers must reconcile the convenience and enhanced capabilities offered by the use of their personal devices for work with their commitment to safeguard their clients’ confidential and sensitive information.

In light of confidential and privileged information on attorneys’ devices, searches of such devices implicate significant “privacy concerns.” *Riley*, 573 U.S. at 386. A client would not expect counsel to leave office doors unlocked, filing cabinets open, correspondence files unattended, or privileged materials strewn across a conference table for government inspection. Yet because modern technology has consolidated the functional equivalent of those spaces onto a single device, a search of an attorney’s cell phone can expose that vast store of confidential client information and privileged communications. Such searches thus jeopardize attorneys’ professional obligations to maintain confidentiality over client information and protect attorney-client privileged information.

Those obligations are related but distinct. The duty of confidentiality broadly protects all information relating to the representation of a client, regardless of source, absent informed client consent or implied authorization. The evidentiary attorney-client privilege,

¹⁵ Steven M. Puiszis, *Can’t Live with Them, Can’t Live without Them—Ethical and Risk Management Issues for Law Firms that Adopt a “BYOD” Approach to Mobile Technology*, 2015 J. Prof. Law. 33, 34 (2015).

in turn, protects a subset of confidential communications between lawyers and clients and their agents, made for the purpose of obtaining or providing legal assistance. These protections exist because clients can obtain meaningful legal advice and lawyers can provide effective representation only when clients are able to communicate fully and candidly with counsel, secure in the knowledge that their confidential information will remain protected.

A. Attorneys Have A Duty To Maintain Confidentiality Over Client Information On Their Devices.

The duty of confidentiality is among the most fundamental obligations imposed upon attorneys. Today, this duty is codified in ABA Model Rule 1.6, which has been adopted in whole or substantial part by most jurisdictions.¹⁶

Under Model Rule 1.6, a lawyer generally “shall not reveal information relating to the representation of a client” absent client consent or implied authorization.¹⁷ As explained in the comments to Rule 1.6, confidentiality is “[a] fundamental principle in the client-lawyer relationship” that “contributes to the trust that is the hallmark of the client-lawyer relationship” and encourages clients “to communicate fully and frankly with the lawyer.”¹⁸ The ethical rule applies to

¹⁶ See *Attorneys’ Duties to Protect Client Data*, Practical Law Practice Note w-014-0379, State Survey: Adopted Duty to Prevent Inadvertent or Unauthorized Disclosure Rule (table reflecting that 46 states have adopted Rule 1.6(c) and/or accompanying comments 18 and 19 in some form).

¹⁷ Model Rules of Pro. Conduct r. 1.6(a) (ABA 1983).

¹⁸ Model Rules of Pro. Conduct r. 1.6 cmt. 2 (ABA 2002).

“all information relating to the representation, whatever its source,” including information that falls outside the attorney-client privilege and work-product doctrine.¹⁹

Rule 1.6 does not only generally prohibit disclosure of client information; it requires attorneys to affirmatively protect it. Rule 1.6(c) directs lawyers to “make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to,” information relating to the representation of a client.²⁰ This obligation works in tandem with Rule 1.1’s requirement that lawyers maintain necessary “knowledge[] and skill,”²¹ which involves “keep[ing] abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology.”²²

In an era when vast quantities of client information are stored electronically, attorneys must understand and address technological risks that may compromise client confidentiality. Failure to do so can carry real consequences, including sanctions and fiduciary-duty claims. *See, e.g., In re Conduct of Conry*, 491 P.3d 42, 57, 60 (Ore. 2021) (publicly reprimanding attorney for “violat[ing] the duty to protect client confidences * * * when he revealed client’s full name in response to [a] negative [online] review[]”); *People v. Braham*, 470 P.3d 1031, 1031 (Colo. 2017) (suspending counsel who “sent two emails to [a] bankruptcy trustee and others in which he disclosed confidential information”);

¹⁹ Model Rules of Pro. Conduct r. 1.6 cmt. 3 (ABA 1983).

²⁰ Model Rules of Pro. Conduct r. 1.6(c) (ABA 1983).

²¹ Model Rules of Pro. Conduct r. 1.1 (ABA 1983).

²² Model Rules of Pro. Conduct r. 1.1 cmt. 8 (ABA 2012).

Hiscox Ins. Co. v. Warden Grier, LLP, 474 F. Supp. 3d 1004, 1008 (W.D. Mo. 2020) (denying motion to dismiss breach of fiduciary duty claim against law firm that failed to protect client information from a cyberattack). More broadly, courts have recognized that technological incompetence can itself constitute professional misconduct, particularly when it impairs an attorney’s ability to meet discovery and other professional obligations. *See, e.g., James v. Nat’l Fin. LLC*, No. 8931-VCL, 2014 WL 6845560, at *12 (Del. Ch. Dec. 5, 2014) (awarding sanctions for discovery misconduct and explaining that under Model Rule 1.1 comment 8, “deliberate ignorance of technology is inexcusable”) (quotation omitted); *DR Distribs., LLC v. 21 Century Smoking, Inc.*, 513 F. Supp. 3d 839, 943, 961 (N.D. Ill. 2021) (quoting the ABA’s Commission on Ethics 20/20’s statement that “[l]awyers must understand technology in order to provide clients with competent and cost effective services” when imposing sanctions for counsel’s failure to collect and disclose electronically stored information).

B. Attorneys Are Under An Obligation To Preserve Privileged Communications On Their Devices.

Certain confidential client information related to the representation of the client receives an additional layer of protection under the attorney-client privilege, which safeguards confidential communications between the attorney and the client made for the purpose of obtaining or providing legal assistance. *See Fisher v. United States*, 425 U.S. 391, 403 (1976); Restatement (Third) of the Law Governing Lawyers § 68 (2000). The attorney-client privilege—which belongs to the client, not the lawyer—is deeply rooted in the

history and tradition of the legal profession. *See The New Wigmore: Evidentiary Privileges* § 3.2.3 (4th ed. 2022) (noting that the privilege dates to sixteenth-century England).

Like an attorney’s broader duty of confidentiality, the attorney-client privilege exists to ensure that clients may seek legal advice without fear that their disclosures will later be revealed to others. *See Commodity Futures Trading Comm’n v. Weintraub*, 471 U.S. 343, 348 (1985). Effective representation requires counsel to be “fully informed by the client.” *Upjohn Co. v. United States*, 449 U.S. 383, 389 (1981); *see also Mohawk Indus., Inc. v. Carpenter*, 558 U.S. 100, 108 (2009). Clients thus must often disclose information spanning every aspect of their lives and affairs, including personal, financial, medical, business, familial, and other sensitive matters. As this Court has long recognized, a strong attorney-client privilege permits and protects such candor. *See Swidler & Berlin v. United States*, 524 U.S. 399, 409 (1998) (holding that application of the privilege should not turn on “[b]alancing *ex post* the importance of the information against client interests”).

In addition to furthering private ends between the attorney and her client, the attorney-client privilege advances the public purposes of fostering “observance” with the law and supporting the “administration of justice.” *Upjohn*, 449 U.S. at 389; *see also Jaffee v. Redmond*, 518 U.S. 1, 11 (1996); *Hunt v. Blackburn*, 128 U.S. 464, 470 (1888). In an age where such communications occur digitally, protecting materials on attorneys’ electronic devices serves the public good.

C. Absent Judicial Supervision, Border Searches Of Attorneys’ Devices Impose Unique Burdens On Attorneys And Their Clients.

When government agents discretionarily access the devices attorneys use to communicate with clients and perform their work, the intrusion threatens the privacy and protections that exist to benefit clients, facilitate legal representation, and promote the fair administration of justice. If clients believe the information entrusted to counsel may be accessed through routine warrantless searches of those devices, then clients very well may hesitate to communicate candidly, and attorneys may be deprived of the information necessary to effectively serve their clients. Worse yet, in light of the amount of confidential and privileged information that may be on any particular device, a warrantless search of even one device may unreasonably expose countless pieces of confidential and/or privileged information to government review.

The unique confidentiality and privacy concerns attendant to searches of attorneys’ devices have compelled the ABA to identify measures legal professionals can take when traveling internationally to help navigate the border-search exception and attorneys’ professional and ethical obligations.²³ The ABA has recommended that traveling lawyers “[c]onsider obtaining a new but inexpensive electronic device” to hold “only necessary information” and “placing

²³ Hon. Daniel J. Crothers & Barbara S. Gillers, *Electronic Device Advisory for Mid-Year Meeting Attendees*, ABA (Jan. 10, 2018), <https://perma.cc/2SQN-CMYA>; see also Pet. 27-28 (discussing “defensive measures” other organizations have developed in light of the border-search exception).

electronic devices in ‘airplane’ mode or having all wi-fi, Bluetooth and cellular connections terminated and disabled” “[b]efore approaching a border inspection area.”²⁴ Privacy experts agree that the border-search exception should make “lawyers * * * extra vigilant about securing protected attorney-client information on their phones and laptops when traveling,” and accordingly take measures like purchasing a “loaner laptop that is ‘clean’ of any client information.”²⁵

These measures are highly unusual and unduly burdensome. “Burner” devices—cheap, anonymized devices—are associated more with drug traffickers than practicing attorneys. *E.g.*, *United States v. Wise*, 74 F.4th 953, 955 (8th Cir. 2023) (explaining that “a ‘burner’ phone * * * is commonly used in drug trafficking to hide the dealer’s identity”). And the use of such devices is burdensome—if not impractical—for many attorneys. Travel-only devices must be purchased, set up, and/or configured for the particular attorney who is using that device, if the device is shared among several at a law firm. Moreover, as explained above, the modern practice of law involves clients who expect to be able to communicate with their attorneys at all times. *See supra* p. 9. Attorneys are also under an

²⁴ Crothers & Gillers, *supra*, at 6-7.

²⁵ Anna Stolley Persky, *As Customs and Border Protection Agents Search More Electronic Devices, How Can Lawyers Keep Client Information Secure?*, 112 ABA, Winter 2026, at 22-23; E. Norman Veasey, *Protection of Client Confidential Information from Cyberattacks Is a Compelling Business and Ethical Priority for inside and outside Corporate Counsel*, 75 Bus. Law. 1495, 1513-14 n.62 (Winter 2019-2020) (“[I]nternational travel can be problematic for the lawyer who brings her smart phone, laptop, or other device containing confidential client information across international borders * * *.”).

obligation to “promptly” communicate with their clients about certain matters, “promptly comply with reasonable requests for information,” and “keep the client reasonably informed about the status of the matter.”²⁶ It should go without saying that an attorney who travels with a device scrubbed of confidential and privileged information may be hindered from meeting these client expectations and professional obligations. Indeed, in light of the fact that lawyers’ electronic devices now may centralize everything about a matter into one device, *see supra* pp. 9-10, parting with that device—even for a few days—can burden attorneys’ fundamental ability to practice.

Making matters worse, commentators have recognized that the steps an attorney may take to minimize the risk of exposing confidential or privileged information can also make that attorney’s device “suspicious.”²⁷ The very actions an attorney may take in light of their obligation “to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client”²⁸ thus may only serve to exacerbate the government’s intrusion into their personal and professional effects.

The division between the circuits aggravates matters further. As Petitioner has explained and as the ABA has long recognized, the circuits are split over how the border-search exception applies to electronic devices. *See* Pet. 9-12; Resolution 19M107A, *supra*,

²⁶ Model Rules of Pro. Conduct r. 1.4(a)(1), (a)(4), (a)(3) (ABA 1983).

²⁷ Persky, *supra*, at 23.

²⁸ Model Rules of Pro. Conduct r. 1.6(c) (ABA 1983).

Report at 6 (“[T]here is now a clear split among federal circuits that should justify intervention by the U.S. Supreme Court.”). This split has significant, and unjustified, real-world consequences. For example, an attorney entering the United States from California is generally protected by a warrant requirement, but an attorney entering from Texas is not. *See* Pet. 9-10. Attorneys, particularly those at large firms, thus must not only juggle the ethical rules of their jurisdiction of licensure,²⁹ but also the particular constitutional rule of their destination.

III. THIS COURT SHOULD RESOLVE THE QUESTION PRESENTED TO PROVIDE NEEDED CLARITY FOR ATTORNEYS AND THEIR CLIENTS.

This case provides an excellent opportunity for this Court to address the question presented and vindicate the substantial privacy and confidentiality interests implicated by searches of electronic devices at the border. The number of electronic devices searched by government agents at the border has skyrocketed in recent years. *See* Pet. 22-23. Consistent with that overall trend, “searches of lawyers’ electronic devices at the border” are “increasingly frequent.”³⁰

The ABA believes that the current state of the law, with the circuits split in multiple ways, is untenable and significantly harms clients’ interests. In 2019, the ABA adopted a Resolution “urg[ing] the federal

²⁹ Crothers & Gillers, *supra* (suggesting that attorneys determine “whether the Rules of Professional Conduct in your jurisdiction of licensure would permit you to consent to a ‘request’ for inspection, or to accede to a ‘demand’”).

³⁰ Resolution 19M107A, *supra*, Report at 9.

judiciary to recognize the substantial privacy and confidentiality interests, as well as the important national security and law enforcement interests, implicated by searches and seizures of electronic devices at the border.”³¹ The ABA’s formal recognition of the fundamental privacy and confidentiality interests at stake during searches of electronic devices at the border builds on its prior advocacy. In 2017, then-ABA President Linda Klein wrote DHS on behalf of the organization’s members to “express concern about maintaining the confidentiality of client information contained in lawyers’ electronic devices” during searches at the border.³² President Klein acknowledged that “security at the nation’s borders is of fundamental importance,” and that attorneys traveling across the border should expect to “become subject to routine searches by CBP and ICE agents.”³³ But President Klein stressed that the critical importance of border security must be weighed against attorneys’ “fundamental” interests in protecting their clients’ confidential information.³⁴

In response to the ABA’s advocacy, CBP, but not ICE, issued a revised Directive addressing how officials should respond when an attorney asserts privilege.³⁵ For example, the revised Directive instructs agents to “segregat[e] * * * privileged material from other information” and states that privileged material

³¹ Resolution 19M107A, *supra*.

³² Klein Letter, *supra*, at 1.

³³ *Id.*

³⁴ *Id.*

³⁵ CBP Directive No. 3340-049A, Border Search of Electronic Devices (Jan. 4, 2018).

“will only be shared with agencies * * * that have mechanisms in place to protect appropriately such information.”³⁶ While commendable, “the Founders did not fight a revolution to gain the right to government agency protocols.” *Riley*, 573 U.S. at 398.

This case presents the opportunity to conclusively resolve this pressing question. Petitioner is an attorney whose work phone—which contained “extremely sensitive information about his clients and their cases, including call logs, voice mails, text message threads with clients, * * * work emails,” and “drafts of confidential filings”—was searched without a warrant over his “vigorous[] protest[s].” Pet. App. 112a-113a. Government agents thus likely had access to—and remain in possession of, *see* Pet. 6—confidential and privileged information.

Such a search strikes at the core of every attorney’s professional obligations and duties. Even more problematic here, Petitioner is an immigration attorney frequently adverse to DHS—meaning that the search of his device may not only have exposed confidential and privileged information, but did so to a litigation adversary. *See* Pet. 24. And in the wake of this search, Petitioner no longer travels with his work phone, Pet. App. 13a, hindering “his ability to remain accessible [to his clients] while abroad,” Pet. 27.

This case is thus a prime example of both the risks of the current border-search regime and the extraordinary and burdensome steps attorneys may take to avoid exposing confidential and/or privileged information to a warrantless search when they re-enter the United States.

³⁶ *Id.* §§ 5.2.1.2, 5.2.4.

CONCLUSION

For the foregoing reasons and those described by Petitioner, the petition for a writ of certiorari should be granted.

Respectfully submitted,

JO-ANN TAMILA SAGAR
MICHAEL J. WEST
JACKSON B. SKEEN
HOGAN LOVELLS
CADWALADER US LLP
555 Thirteenth St., N.W.
Washington, D.C. 20004

ERICA J. SHULER
HOGAN LOVELLS
CADWALADER US LLP
8350 Broad St., Floor 17
Tysons, VA 22102

BARBARA J. HOWARD
Counsel of Record
PRESIDENT
AMERICAN BAR ASSOCIATION
321 N. Clark St.
Chicago, IL 60654
312-988-5000
amicusbriefs@americanbar.org

Counsel for Amicus Curiae American Bar Association

SEPTEMBER 2026