107A

AMERICAN BAR ASSOCIATION

SECTION OF CIVIL RIGHTS AND SOCIAL JUSTICE
CRIMINAL JUSTICE SECTION

REPORT TO THE HOUSE OF DELEGATES

RESOLUTION

RESOLVED, That the American Bar Association urges the federal judiciary to recognize the substantial privacy and confidentiality interests implicated by searches and seizures of electronic devices at the border; and

FURTHER RESOLVED, That the American Bar Association urges Congress to enact legislation and, until legislation is enacted, urges the U.S. Department of Homeland Security to adopt policy, that would:

(1) require a warrant based on probable cause for seizures (other than temporary seizures for the purpose of obtaining a warrant) and searches of electronic devices carried by individuals at the border;
(2) prohibit any government entity from denying a lawful permanent resident entry or exit based on the person's failure to disclose an access credential or provide access to an electronic device for a search;
(3) implement policies and procedures to preserve the attorney-client privilege, the work product doctrine, and the lawyer's ethical obligation to maintain confidential information during border crossings; and
(4) require the government to record each instance in which it conducts a search of an electronic device seized at the border and issue an annual report summarizing such searches.

107A

REPORT

Summary

This resolution calls on the federal judiciary, Congress, and the Department of Homeland Security to protect the privacy of millions of individuals who cross our nation's borders each year.

Introduction

Over the last ten years, the Supreme Court has twice affirmed that the digital records we each create, store, and transport every day are entitled to protection under the Fourth Amendment. First, the Court in *Riley v. California* rejected decades of precedent and held that a search of a cell phone requires a warrant even when that search is incident to arrest, because of the quantity, quality, and uniquely sensitive nature of the personal data stored on those devices.[1] Then the Court in *Carpenter v. United States* found that cell phone location data, even data held by third party service providers, is also protected and cannot be obtained without a warrant based on probable cause.[2] Meanwhile, millions of individuals cross into and out of the United States each year, and neither the Supreme Court nor Congress has addressed the proper degree of protection needed for searches of electronic devices at the border.

The traditional Fourth Amendment rule permitted warrantless searches at the border.[3] But, even before the Supreme Court issued its decision in *Riley,* federal appellate courts recognized that searches of electronic devices implicate significant privacy interests that justify greater protection.[4] Since then, the problem has become more acute as the use of smartphones has proliferated. Today, individuals rely on their phones and other electronic devices to engage in personal, professional, educational, political, and spiritual pursuits; nearly every activity—from the most mundane to the most significant and private—can and is being done through or with the use of an electronic device. Searches of these devices, as the Supreme Court has explained, implicate the most intimate details of our lives and should be appropriately limited.

Over the last forty years, the ABA has adopted policies supporting greater privacy protection and urging Congress and the courts to protect individual rights.[5] The ABA has identified and on numerous occasions urged Congress to address new privacy risks

---

[1] *Riley v. California*, 134 S. Ct. 2473 (2013); *see also* Alan Butler, *Get A Warrant: The Supreme Court's New Course for Digital Privacy Rights After* Riley v. California, 10 Duke J. Const. L. & Pub. Pol'y 83 (2014).
[2] *Carpenter v. United States*, 138 S. Ct. 2206 (2018).
[3] *See United States v. Ramsey*, 431 U.S. 606 (1977) (finding that border searches fall within a "historically recognized exception to the Fourth Amendment's general principle that a warrant be obtained").
[4] *See, e.g.*, *United States v. Cotterman*, 709 F.3d 952 (9th Cir. 2013), *cert. denied* 561 U.S. 1156 (2014).
[5] *See* ABA Section of Civil Rights and Social Justice, Privacy and Information Protection Commission, *ABA Policies Relating to Privacy and Information Protection* (Sept. 25, 2018), http://apps.americanbar.org/webupload/commupload/IR511000/relatedresources/ABA-Privacy-Policies-CRSJ-PIP-09252018.pdf.

posed by emerging technologies. Specifically, the ABA advocated for important privacy law updates including enactment of the Electronic Communications Privacy Act (ECPA),[6] amendments to the Privacy Act,[7] enactment of legislation protecting the privacy of medical records,[8] and updates to ECPA reflecting technological and societal changes.[9] The ABA has also underscored the significant threat that unchecked searches of electronic devices can have on the confidentiality of attorney-client communications and work product. Specifically, last year the ABA President wrote to the Secretary of Homeland Security to express concerns over standards for searches of electronic devices without reasonable suspicion, and how those searches impact lawyers' confidential records.[10]

This resolution establishes that the American Bar Association supports the rights of individuals to be free from warrantless searches and seizures[11] of their electronic devices at the border,[12] and urges the Federal Judiciary, Congress, and the Department of Homeland Security to recognize the important privacy interests at stake and to establish necessary legal protections. Specifically, the resolution establishes that the American Bar Association supports a warrant based on probable cause standard for certain searches and seizures of electronic devices carried by individuals at the border. As this report recognizes, the traditional warrant standard is subject to a number of exceptions depending on the context of the search; the purpose of this resolution is to establish that the traditional exception to the warrant requirement for searches conducted at the border should not apply to searches of electronic devices carried by individuals. We recognize that other exceptions may still apply depending on the exact circumstances of a particular search. This report and resolution does not address such other circumstances.

---

[6] ABA Report and Recommendation 86A114B, https://www.americanbar.org/content/dam/aba/administrative/crsj/committee/aug-86-wiretap-law.authcheckdam.pdf.

[7] ABA Report and Recommendation 86A114C, https://www.americanbar.org/content/dam/aba/administrative/crsj/committee/aug-86-electronic-communication-on-privacy.authcheckdam.pdf.

[8] ABA Report and Resolution 96M106, https://www.americanbar.org/content/dam/aba/directories/policy/1996_my_106.authcheckdam.pdf; ABA Report and Resolution 99M109A, http://www.americanbar.org/content/dam/aba/directories/policy/1999_my_109a.authcheckdam.pdf.

[9] ABA Report and Resolution 13A114, https://www.americanbar.org/content/dam/aba/administrative/crsj/committee/aug-13-electronic-communication-act.authcheckdam.pdf.

[10] Letter from Linda Klein, President, Am. Bar Ass'n, to Gen. John F. Kelly, USMC (Ret.), Sec'y of Homeland Sec., U.S. Dep't of Homeland Sec. (May 5, 2017), https://www.americanbar.org/content/dam/aba/images/government_affairs_office/attyclientprivissue(bordersearchesofattorneydevices,abalettertodhs,finalversion,may5,2017).pdf.

[11] The term "seizure" in the resolution does not include temporary seizures conducted as part of a physical inspection of a device at the border or temporary seizures necessary to obtain a warrant.

[12] The term "forensic search" was explained by the Ninth Circuit in *United States v. Cotterman*, 709 F.3d 952, 968 (9th Cir. 2013) (en banc) and has been defined more specifically in the Leahy-Daines bill now being considered by the U.S. Senate, S. 2462, 115th Cong. §1 (2018). This resolution does not track the forensic / non-forensic search distinction drawn in these cases. Instead, it distinguishes between searches of electronic devices vs. physical inspections or temporary seizures of those devices under the standard explained by the Court in *Riley*.

Fourth Amendment Protections for Electronic Devices

The Fourth Amendment provides that:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[13]

The Supreme Court has established that "in the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement."[14] For example, the Court has long recognized an exception to the warrant requirement in a range of exigent circumstances and emergencies.[15] The Court has also recognized a narrow exception for warrantless searches at the border. Specifically, the Court has held that because the "Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border,"[16] searches are typically found to be "reasonable simply by virtue of the fact that they occur at the border."[17] But even at the border, the Court has held, the Fourth Amendment is not a dead letter; individual privacy rights are to be "[b]alanced against the sovereign's interests."[18] The Supreme Court has never had occasion to consider the balance of interests at stake during the search of an individual's electronic devices at the border.

The Supreme Court has recently considered the privacy interests implicated by searches of electronic devices in other contexts, and has twice held that such searches must be strictly limited. First, in *Riley v. California*, 134 S. Ct. 2473 (2013), the Court held that the long-standing exception permitting warrantless searches incident to arrest did not apply to a search of a cell phone seized during an arrest. Chief Justice Roberts, writing for a unanimous Court, found that the traditional exception did not apply to searches of cell phones, which "place vast quantities of personal information literally in the hands of individuals," and found that searches of these devices "bear[] little resemblance to the type of brief physical search considered" in prior cases.[19] The Court found that cell phones

---

[13] U.S. Const. amend. IV.
[14] *Carpenter*, 138 S. Ct. at 2221.
[15] *See Missouri v. McNeely*, 569 U.S. 141, 149 (2013) (discussing the traditionally recognized exigency exceptions). The Supreme Court has so far not resolved whether there is a "foreign intelligence exception" to the warrant requirement, but lower courts have recognized a limited exception in some circumstances. *See United States v. United States District Court (Keith)*, 407 U.S. 297, 321–23 (1972) (refusing to recognize a general domestic security exception to the warrant requirement, without expressing an "opinion as to, the issues which may be involved with respect to activities of foreign powers or their agents."); *In re Terrorist Bombings of U.S. Embassies in East Africa*, 552 F.3d 157, 172 (2d Cir. 2008) (discussing cases that have recognized a limited exception to the warrant requirement for foreign intelligence searches).
[16] *United States v. Flores-Montano*, 541 U.S. 149 (2004).
[17] *Ramsay*, 431 U.S. at 616.
[18] *United States v. Montoya de Hernandez*, 473 U.S. 531, 539 (1985).
[19] 134 S. Ct. at 2484.

"differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person."[20] Quoting Learned Hand, the Court emphasized "that it is 'a totally different thing to search a man's pockets and use against him what they contain, from ransacking his house for everything which may incriminate him'" but noted that is no longer true "[i]f his pockets contain a cell phone."[21] Searching a cell phone "would typically expose to the government far *more* than the most exhaustive search of a house . . . [a phone] contains a broad array of private information never found in a home in any form—unless the phone is."[22] The Court noted that "[l]aw enforcement officers remain free to examine the physical aspects of a phone to ensure that it will not be used as a weapon—say, to determine whether there is a razor blade hidden between the phone and its case."[23]

More recently, in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), the Court held that the "third party doctrine"—under which courts had held that certain records held by service providers, banks, and other third parties were not entitled to Fourth Amendment protection—does not apply to cell phone location data. Specifically, the Court held that historical cell phone location records held by a wireless carrier were protected under the Fourth Amendment and the Government could not obtain them without a warrant. The Court found that cell phone location records were "qualitatively different" from the "telephone numbers and bank records" that the Court held could be obtained without a warrant in *Smith* and *Miller*.[24] The Court noted that "few could have imagined" in the 1970s "a society in which a phone goes wherever its owner goes, conveying to the wireless carrier not just dialed digits, but a detailed and comprehensive record of the person's movements."[25] As in *Riley*, the Court emphasized the "novel circumstances" regarding searches of electronic devices due to the sheer quantity and unique quality of the data that can be obtained. The Court also indicated that its decision "does not consider other collection techniques involving foreign affairs or national security."[26]

Fourth Amendment Border Search Cases Prior to *Riley* and *Carpenter*

Even before the Supreme Court imposed special limitations on searches of cell phones, lower courts had recognized the need to limit certain searches of electronic devices at the border. Though courts have traditionally permitted suspicionless searches and seizures at the border, the U.S. Court of Appeals for the Ninth Circuit held in *United States v. Cotterman*, 709 F.3d 952 (9th Cir. 2013) (en banc), that a "forensic examination" of an individual's laptop seized at the border was not permissible under the Fourth Amendment

[20] Id. at 2489.
[21] Id. at 2490–91 (quoting *United States v. Kirschenblatt*, 16 F.2d 202, 203 (2d Cir. 1926)).
[22] Id. at 2491 (emphasis in original).
[23] Id. at 2485.
[24] *Carpenter v. United States*, 138 S. Ct. 2206, 2216 (2018); *see Smith v. Maryland*, 442 U.S. 735 (1979) (holding that an individual did not have a reasonable expectation of privacy in records of telephone numbers that they conveyed to the phone company when they dialed); *Miller v. United States*, 425 U.S. 435 (1976) (holding that an individual did not have a reasonable expectation of privacy in financial records held by a bank).
[25] *Carpenter*, 138 S. Ct. at 2217.
[26] *Id*. at 2220.

unless the Government had reasonable suspicion to support the search.[27] The court did not specifically define the term forensic examination, but noted the search involved the use of "forensic software to copy the hard drive and then analyze it in its entirety, including data that ostensibly had been deleted."[28] The court also noted that the software "exhibited the distinctive features of computer forensic examination" because it "copied, analyzed, and preserved the data stored on the hard drive and gave the examiner access to far more data, including password-protected, hidden or encrypted, and deleted files, than a manual user could access."[29]

The Ninth Circuit in *Cotterman* found that although "[i]nternational travelers certainly expect that their property will be searched at the border," they do not expect "that, absent some particularized suspicion, agents will mine every last piece of data on their devices or deprive them of their most personal property for days (or perhaps weeks or even months, depending on how long the search takes)."[30] The court explained that this standard was necessary given the "substantial personal privacy interests" at stake because "the private information individuals store on digital devices—their personal 'papers' in the words of the Constitution—stands in stark contrast to the generic and impersonal contents" of other containers that the Government has authority to search.[31] The court further emphasized the vast quantity and unique qualities of personal information stored on these devices.[32]

Prior to the Ninth Circuit's decision in *Cotterman*, courts had already required reasonable suspicion for "extended border searches" of any property.[33] But the standard for searching traditional physical property was flexible to reflect the "myriad difficulties facing customs and immigration officials who are charged with the enforcement of smuggling and immigration laws."[34] The Ninth Circuit had accordingly defined an extended border search as any "search away from the border where entry is not apparent."[35] These searches occur "after the actual entry has been effected and intrude more on an individual's normal expectation of privacy," which is why courts have required that the government first establish reasonable suspicion "that the subject of the search was involved in criminal activity."[36] The Ninth Circuit's decision in *Cotterman* recognized that some searches of electronic devices require reasonable suspicion even if they do not qualify as an "extended border search."[37]

---

[27] *United States v. Cotterman*, 709 F.3d 952, 968 (9th Cir. 2013) (en banc).
[28] *Id*. at 962.
[29] *Id*. at 963 n.9.
[30] *Id*. at 967.
[31] *Id*. at 964.
[32] *Id*.
[33] *See United States v. Stewart*, 715 F. Supp. 2d 750, 753–54 (E.D. Mich. 2010) (discussing earlier cases on the "extended border search" standard); *United States v. Guzman-Padilla*, 573 F.3d 865, 877–87 (9th Cir. 2009); *United States v. Niver*, 689 F.2d 520, 526 (5th Cir. 1982).
[34] *Guzman-Padilla*, 573 F.3d at 878 (quoting *United States v. Richards*, 638 F.3d 765, 771 (1981)).
[35] *Id*. at 878 (quoting *United States v. Corral-Villavicencio*, 753 F.2d 785, 788 (9th Cir. 1985)).
[36] *Id*. at 877–78.
[37] *Cotterman*, 709 F.3d at 961.

107A

In the five years since *Cotterman*, many more federal district and appellate courts have grappled with forensic examinations of electronic devices at the border.[38] Several Courts of Appeals have weighed in and come down on different sides. Following recent decisions, there is now a clear split among federal circuits that should justify intervention by the U.S. Supreme Court. The Fourth Circuit held in *United States v. Kolsuz*, 890 F.3d 133 (4th Cir. 2018), that the *Cotterman* standard applies and reasonable suspicion is required to conduct a forensic examination of a cell phone seized at the border. The Eleventh Circuit disagreed in *United States v. Touset*, 890 F.3d 1227 (11th Cir. 2018), holding that the Fourth Amendment does not require any suspicion for forensic searches of electronic devices at the border. Several other decisions have touched on this issue, but those cases did not provide the best active vehicle for the Court's consideration.[39] Given the circumstances, there is a significant possibility that the Court will weigh in on this issue soon (if not in *Touset,* then in another similar case).

The Supreme Court established in *Riley* and *Carpenter* that electronic devices (cell phones, in particular) contain large volumes of uniquely sensitive personal information. Due to the "seismic shifts in digital technology" that have occurred over the last two decades, the Court has found that certain traditional Fourth Amendment exceptions do not adequately protect reasonable expectations of privacy when applied to these electronic devices. The same logic applies to extended seizures and forensic searches of electronic devices at the border. Even before *Riley* and *Carpenter*, courts had begun to recognize that suspicionless forensic searches of electronic devices at the border were not reasonable and thus violated the Fourth Amendment. Now, after *Riley* and *Carpenter*, the Court should make clear that extended seizures and forensic searches of cell phones and other electronic devices at the border are not reasonable absent probable cause that the subject was involved in criminal activity.[40] Congress should also take action to impose

---

[38] *See, e.g.*, *Alasaad v. Nielsen*, 2018 WL 2170323, No. 17-11720 (D. Mass. May 9, 2018) (denying the Government's motion to suppress a civil rights suit challenging searches and seizures of electronic devices at the border); *United States v. Kim*, 103 F. Supp. 3d 32 (D.D.C. 2015) (granting a motion to suppress evidence gathered during a warrantless search of a laptop by border patrol agents following seizure at a U.S. airport); *United States v. Saboonchi*, 990 F. Supp. 2d 536 (D. Md. 2014) (imposing a reasonable suspicion standard for the search of a laptop); *United States v. Hassanshah*, 75 F. Supp. 3d 101 (D.D.C. 2014) (same); *Abidor v. Napolitano*, 990 F. Supp. 2d 260 (E.D.N.Y. 2013) (rejecting challenge to forensic searches of electronic devices where the court found that the government had reasonable suspicion).

[39] The Court recently denied a Petition for a Writ of Certiorari in *United States v. Vergara*, 884 F.3d 1309 (11th Cir. 2018), *cert. denied* ___ S. Ct. ___, 2018 WL 1993728 (Mem) (No. 17-8639) (Oct. 1, 2018), which involved a similar question but may not have been an ideal vehicle for the Court's consideration. The Sixth Circuit ruled against a defendant's challenge to a laptop search in *United States v. Stewart*, 729 F.3d 517 (6th Cir. 2013), based on a finding that border agents only subjected his computer to a "routine" and "non-forensic examination." *Id*. at 525. The Fifth Circuit more recently ruled against a Defendant in *United States v. Molina-Isidoro*, 884 F.3d 287 (5th Cir. 2018), based on a finding that agents had probable cause to conduct a forensic search of her cell phone. *Id*. at 291. The defendant in *Kolsuz* was unsuccessful in obtaining a suppression remedy, despite the favorable ruling on the Fourth Amendment standard, and appears to have decided not to file a Petition for Writ of Certiorari. It appears that the defendant in *Touset* has also chosen not to file a Petition for Writ of Certiorari.

[40] The difficulties involved in border enforcement may justify properly predicated searches conducted without first obtaining a judicially-authorized warrant under the Federal Rules of Criminal Procedure.

more specific restrictions and guidelines concerning searches of electronic devices at the border.

Legislative Interest in the Border Search Issue

Court consideration of the appropriate Fourth Amendment standard for forensic searches of electronic devices at the border is necessarily limited. Judicial review typically only arises following a criminal indictment via a motion to suppress evidence gathered during the search, and possibly as an issue in an appeal following conviction. Many searches conducted do not lead to a criminal indictment or even any evidence of a potential crime. But the individuals subjected to these searches are nevertheless deprived of the use of their devices and are subjected to the arbitrary search of their "papers" by Government agents. Recent reports show that U.S. Customs agents are increasingly scrutinizing personal devices, with a 60% increase in fiscal year 2017.[41] Other countries have taken even more draconian approaches, including a new customs rule in New Zealand that subjects travelers to a $5,000 NZD fine if they refuse to turn over passwords or other information enabling access to their electronic devices.[42]

Against the backdrop of this expansion of border searches, members of Congress have called for legislative action. In the spring of 2017, Senator Ron Wyden (D-OR) introduced the "Protecting Data at the Border Act," which was co-sponsored by Senator Rand Paul (R-KY), Senator Edward Markey (D-MA), and Senator Jeff Merkley (D-OR).[43] The Wyden-Paul bill would prohibit a government entity from accessing "the digital contents of any electronic equipment belonging to or in the possession of a United States person at the border without a valid warrant supported by probable cause," and from denying "entry into or exit from the United States by a United States person based on refusal" to "disclose an access credential" or provide "access to the digital contents of electronic equipment" or to "online account information."[44] The bill would provide for an emergency and "public safety and health" exception to the warrant standard, limit retention of digital contents accessed, impose recordkeeping and audit requirements for electronic device searches at the border, limit seizure of devices, and restrict use of unlawfully obtained evidence.[45]

More recently, Senator Leahy (D-VT) introduced a bill "to place restrictions on searches and seizures of electronic devices at the border," which was co-sponsored by Senator

---

[41] Nick Miroff, *U.S. Customs Agents Are Searching More Cellphones—Including Those Belonging to Americans*, Wash. Post. (Jan. 5, 2018), https://www.washingtonpost.com/world/national-security/us-customs-agents-are-searching-more-cellphones--including-those-belonging-to-americans/2018/01/05/0a236202-f247-11e7-b3bf-ab90a706e175_story.html.
[42] Isaac Stanley-Becker, *New Zealand's 'Digital Strip Searches': Give Border Agents Your Passwords or Risk a $5,000 Fine*, Wash. Post (Oct. 2, 2018), https://www.washingtonpost.com/news/morning-mix/wp/2018/10/02/new-zealands-digital-strip-searches-give-border-agents-your-device-passwords-or-risk-a-5000-fine/.
[43] S. 823, 115th Cong. (2017).
[44] *Id.* § 5.
[45] *Id.* §§ 5–8.

Daines (R-MT).[46] The Leahy-Daines bill would impose strict limits on the ability of Department of Homeland Security officials to "search or seize an electronic device transported by a United States person at the international border."[47] The bill would distinguish between "manual searches," "seizures," and "forensic searches," and impose different restrictions on each category.

The bill would limit any "manual search" of an electronic device by requiring reasonable suspicion that the individual transporting the device "is carrying contraband or is otherwise transporting goods or persons in violation of the laws enforced by the Department of Homeland Security" or is "inadmissible or otherwise not entitled to enter the United States under such laws" and that the device "contains information or evidence relevant to" the violation at issue.[48] The bill defines "manual search" as any examination of an electronic device "conducted manually without (A) the assistance of any other electronic device, electronic equipment, or software, including the use of special search programs; or (B) the entry of any password, passcode, fingerprint, account information, or other biometric identifier that permits access to data otherwise protected by technological means."[49] The bill would also limit seizures of electronic devices by requiring probable cause to believe the same facts about the individual and device described above (or that the individual has violated "any Federal or State law punishable by more than 1 year").[50]

The Leahy-Daines bill would only permit forensic searches of electronic devices pursuant to a warrant issued under the Federal Rules of Criminal Procedure. A "forensic search" is defined in the bill as any examination of an electronic devices that "(A) is conducted for longer than 4 hours; (B) is conducted with the assistance of any other electronic device, electronic equipment, or software, including software enabling the searching, scanning, or indexing of the contents of the device; (C) involves the copying or documentation of the data stored on the device; or (D) is conducted in any other manner that would not fall within the definition of a manual search or [a search subject to another established Fourth Amendment exception."[51] The bill would also prohibit introduction of unlawfully obtained evidence, provide detailed procedures governing searches and seizures of devices at the border, and impose reporting requirements.[52]

Both bills have been referred to the Senate Committee on Homeland Security and Governmental Affairs. There has not yet been a markup or further consideration of the proposals.

Recent Statement by the ABA President on Border Searches

The ABA has already spoken out about the increasingly frequent searches of electronic devices at the border. Although there is no existing ABA policy on the broad Fourth

[46] S. 2462, 115th Cong. (2018).
[47] *Id.* § 2.
[48] *Id*. § 2(b).
[49] *Id*. § 1(2).
[50] *Id.* § 2(c).
[51] *Id*. § 1(1).
[52] *Id.* § 2–4.

Amendment questions, these searches can implicate the confidentiality of attorney-client communications and work product. In 2017, then ABA President Linda Klein wrote to the Secretary and Acting General Counsel of the Department of Homeland Security expressing "serious concerns regarding the standards that permit U.S. Customs and Border Protection ('CBP') and Immigration and Customs Enforcement ('ICE') officers to search and review the contents of lawyers' laptop computers, cell phones, and other electronic devices at U.S. border crossings without any showing of reasonable suspicion."[53]

President Klein relayed and underscored concerns from ABA members about "maintaining the confidentiality of client information contained in lawyers' electronic devices when re-entering the United States," and called on the agency to "ensure that the proper policies and procedures are in place" at DHS, CBP, and ICE to "preserve the attorney-client privilege, the work product doctrine, and the confidentiality of lawyer and client communications during border crossings and to prevent the erosion of these important legal principles."[54] President Klein emphasized that the confidentiality of the lawyer-client relationship is a "cornerstone of our legal system" and is enshrined in ABA Model Rule of Professional Conduct 1.6(a), which states that "a lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent . . . ."[55] President Klein also noted that the ABA has on multiple occasions "fought to preserve" these interests in response to Government surveillance, including in communications to the "then-Director and General Counsel of the National Security Agency" in 2014 concerning "'minimization procedures' [to] protect the confidentiality and attorney-client privileged status of lawyer-client communications intercepted or otherwise received by the NSA or other agencies."[56]

President Klein's letter focused specifically on key provisions in the CBP and ICE policies governing searches of lawyers' and other travelers' electronic devices at the U.S. border. Section 5.2 of CBP Directive No. 3340-049 ("Border Search of Electronic Devices Containing Information") and Sections 6.1 and 8.6 of ICE Directive No. 7-61 ("Border Searches of Electronic Devices"). She noted that both directives "have resulted in" agents "exercising sweeping powers to search electronic devices at the border, with or without reasonable suspicion of any wrongdoing."[57] She also noted that while other provisions may require "special review and handling of privileged or sensitive materials," the concern

---

[53] Letter from Linda Klein, President, Am. Bar Ass'n, to Gen. John F. Kelly, USMC (Ret.), Sec'y of Homeland Sec., and Joseph B. Maher, Acting Gen. Counsel, Dep't of Homeland Sec. (May 5, 2017), *available at* https://www.americanbar.org/content/dam/aba/images/government_affairs_office/attyclientprivissue(bordersearchesofattorneydevices,abalettertodhs,finalversion,may5,2017).pdf.

[54] *Id.*

[55] *Id.*

[56] *Id.* at 2 (citing the ABA' February 2014 letter to the NSA, *available at* https://www.americanbar.org/content/dam/aba/uncategorized/GAO/2014feb20_nsainterceptionofprivileged info_l.authcheckdam.pdf).

[57] *Id.* at 2.

is these other provisions "are not sufficiently clear or comprehensive enough to protect these fundamental legal rights."[58]

President Klein urged the Department to "modify and clarify" the CBP and ICE directives "to emphasize and protect these fundamental legal rights and to provide your front line agents and officers with explicit guidance as to the importance of these principles."[59] She further urged the Department to "revise these Directives to clarify the specific standards and procedures that CBP and ICE agents must follow before the contents of a lawyer's electronic device can be searched or seized at the border."[60]

In response to President Klein's letter, senior officials at the Department of Homeland Security met with the ABA and subsequently issued a revised directive for CBP, which addressed how border officials should respond to assertions that material is privileged.[61] This included specific procedures for approval of such searches, segregation and subsequent disposal of privileged material, and other general limitations on electronic device searches at the border. The revised CBP directive adopts the *Cotterman* standard that an "advanced search" can only be performed if there is reasonable suspicion of unlawful activity or national security concerns.[62] In 2018, ABA President Hilarie Bass stated that the "ABA will continue to urge DHS, CPB (sic), and other agencies to further improve their policies by requiring border officers to obtain a subpoena based on reasonable suspicion or a warrant supported by probable cause before searching the contents of lawyer electronic devices."[63]

Conclusion

Searches of electronic devices at the border implicate significant privacy interests and should be limited both by the Fourth Amendment and by statute. The American Bar Association has previously fought to protect individuals from arbitrary searches of their electronic devices at the border out of concern for the risk to lawyer-client confidentiality, the attorney-client privilege, and the work product doctrine. But more is needed to ensure that the fundamental privacy rights of individuals are protected.

Accordingly, the American Bar Association urges the federal judiciary to recognize the substantial privacy interests implicated by searches of electronic devices at the border. The American Bar Association also urges Congress to enact legislation—and in the meantime for the Department of Homeland Security to adopt policies—that would protect

---

[58] *Id*. at 3.
[59] *Id.* at 4.
[60] *Id.*
[61] Lee Rawles, *Traveling Lawyers Get New Protections in Device Searches at Border*, ABA Journal (Jan. 25, 2018), http://www.abajournal.com/news/article/new_guidelines_for_electronic_device_searches_at_us_borders_will_impact_att.
[62] *See* U.S. Customs and Border Protection, CBP Directive No. 3340-049A (Jan. 4, 2018), *available at* https://www.cbp.gov/sites/default/files/assets/documents/2018-Jan/CBP-Directive-3340-049A-Border-Search-of-Electronic-Media-Compliant.pdf.
[63] Rawles, *supra*.

these substantial privacy interests by imposing a probable cause warrant standard for searches and seizures of electronic devices at the border, protecting against improper denial of entry to gain access to electronic devices, setting standards to protect the attorney-client privilege, the work product doctrine, and the confidentiality of the lawyer-client relationship, and requiring recordkeeping and auditing of border searches.

Respectfully submitted,

Wilson Adam Schooley
Chair, Section of Civil Rights and Social Justice
January 2019

107A

GENERAL INFORMATION FORM

Submitting Entity: Section of Civil Rights and Social Justice

Submitted By: Wilson A. Schooley, Chair, Section of Civil Rights and Social Justice

1. Summary of Resolution(s). This resolution calls on the federal judiciary, Congress, and the Department of Homeland Security to protect the privacy of millions of individuals who cross our nation's borders each year.

2. Approval by Submitting Entity. The Council of the Section of Civil Rights and Social Justice approved sponsorship of the Resolution during its Fall Meeting on Friday, October 12, 2018. The Council of the Criminal Justice Section approved co-sponsorship of the Resolution during its Fall Meeting on Saturday, November 3, 2018.

3. Has this or a similar resolution been submitted to the House or Board previously? No.

4. What existing Association policies are relevant to this Resolution and how would they be affected by its adoption? Over the last forty years, the ABA has adopted policies supporting greater privacy protection and urging Congress and the courts to protect individual rights.[64] The ABA has identified and on numerous occasions urged Congress to address new privacy risks posed by emerging technologies. Specifically, the ABA advocated for important privacy law updates including enactment of the Electronic Communications Privacy Act (ECPA),[65] amendments to the Privacy Act,[66] enactment of legislation protecting the privacy of medical records,[67] and updates to ECPA reflecting technological and societal changes.[68] The ABA has also underscored the significant threat that unchecked searches of electronic devices can have on the confidentiality of attorney-client communications and work product.

---

[64] *See* ABA Section of Civil Rights and Social Justice, Privacy and Information Protection Commission, *ABA Policies Relating to Privacy and Information Protection* (Sept. 25, 2018), http://apps.americanbar.org/webupload/commupload/IR511000/relatedresources/ABA-Privacy-Policies-CRSJ-PIP-09252018.pdf.

[65] ABA Report and Recommendation 86A114B, https://www.americanbar.org/content/dam/aba/administrative/crsj/committee/aug-86-wiretap-law.authcheckdam.pdf.

[66] ABA Report and Recommendation 86A114C, https://www.americanbar.org/content/dam/aba/administrative/crsj/committee/aug-86-electronic-communication-on-privacy.authcheckdam.pdf.

[67] ABA Report and Resolution 96M106, https://www.americanbar.org/content/dam/aba/directories/policy/1996_my_106.authcheckdam.pdf; ABA Report and Resolution 99M109A, http://www.americanbar.org/content/dam/aba/directories/policy/1999_my_109a.authcheckdam.pdf.

[68] ABA Report and Resolution 13A114, https://www.americanbar.org/content/dam/aba/administrative/crsj/committee/aug-13-electronic-communication-act.authcheckdam.pdf.

Specifically, the ABA President in 2017 wrote to the Secretary of Homeland Security to express concerns over standards for searches of electronic devices without reasonable suspicion and how those searches impact lawyers' confidential records.[69] The American Bar Association has a long tradition of advocating for the protection of personal privacy and constitutional rights, and has also fought to protect the confidentiality of the lawyer-client relationship, which is a "cornerstone of our legal system" and is enshrined in ABA Model Rule of Professional Conduct 1.6(a).

5. If this is a late report, what urgency exists which requires action at this meeting of the House? N/A

6. Status of Legislation. In the 115th Congress, two bipartisan bills were introduced in the Senate on this issue—S. 823 (Wyden-Paul) and S. 2462 (Leahy-Daines). Both bills were referred to the Senate Committee on Homeland Security and Governmental Affairs. There has not yet been a markup or further consideration of the proposals.

7. Brief explanation regarding plans for implementation of the policy, if adopted by the House of Delegates. We will work with the ABA Amicus Committee to draft and file an amicus brief in cases involving Fourth Amendment challenges to suspicionless searches of electronic devices at the border. In particular, we will work to file a brief in the *Touset* case (either at the Certiorari stage if time permits, or at the merits stage if the Court grants Certiorari). We will also work with the legislative affairs office to lobby Congress in support of legislation that is consistent with this policy (including both bills currently pending in the Senate).

8. Cost to the Association. (Both direct and indirect costs) Adoption of this proposed resolution would result in only minor indirect costs associated with Section staff time devoted to the policy subject matter as part of the staff members' overall substantive responsibilities.

9. Disclosure of Interest. (If applicable) There are no known conflicts of interest.

10. Referrals. The Report with Recommendation will be referred to the following entities in the month of October:

    Criminal Justice Section
    Science & Technology Law
    Standing Committee on Law and National Security
    General Practice, Solo and Small Firm Section
    Section of International Law

[69] Letter from Linda Klein, President, Am. Bar Ass'n, to Gen. John F. Kelly, USMC (Ret.), Sec'y of Homeland Sec., U.S. Dep't of Homeland Sec. (May 5, 2017), https://www.americanbar.org/content/dam/aba/images/government_affairs_office/attyclientprivissue(borderssearchesofattorneydevices,abalettertodhs,finalversion,may5,2017).pdf.

107A

Judicial Division
Law Student Division
Senior Lawyers Division
Young Lawyers Division

11. Contact Name and Address Information. (Prior to the meeting. Please include name, address, telephone number and e-mail address)

    Alan Butler
    (Chair, CRSJ Committee on Privacy and Information Protection)
    Senior Counsel, Electronic Privacy Information Center
    1718 Connecticut Ave. NW, Suite 200
    Washington, DC 20009
    Tel.: (202) 483-1140
    Email: butler@epic.org

    Paula Shapiro, Acting Director
    Section of Civil Rights and Social Justice
    1050 Connecticut Avenue NW
    Washington, DC 20036
    Tel: (202) 662-1029
    Email: Paula.Shapiro@americanbar.org

12. Contact Name and Address Information. (Who will present the report to the House? Please include name, address, telephone number, cell phone number and e-mail address.)

    Estelle H. Rogers, CRSJ Section Delegate
    111 Marigold Ln
    Forestville, CA 95436-9321
    Tel.: (202) 337-3332 (Work)
    E-mail: 1estellerogers@gmail.com

    Mark I. Schickman, CRSJ Section Delegate
    Freeland Cooper & Foreman LLP
    150 Spear Street, Suite 1800
    San Francisco, CA
    Tel.: (415) 541-0200
    E-mail: schickman@freelandlaw.com

EXECUTIVE SUMMARY

1. Summary of the Resolution

This resolution calls on the federal judiciary, Congress, and the Department of Homeland Security to protect the privacy of millions of individuals who cross our nation's borders each year.

2. Summary of the Issue that the Resolution Addresses

The right to be free from unreasonable searches and seizures is fundamental to the American constitutional structure. The widespread adoption of modern communications technologies has made it possible to travel with constant access to personal and professional contacts, and to maintain constant access to vast quantities of information—from the most sensitive and confidential communications to the more mundane and routine records. The proliferation of cell phones and other electronic devices that enable individuals to carry personal information with them, wherever they go, has significant implications for privacy law. In particular, old rules governing searches of persons and property do not take into account these recent technological changes.

Searches conducted at the international border now implicate significant privacy interests given the volume and sensitivity of records stored on and accessible via electronic devices. Given the Supreme Court's recent rulings expanding the scope of Fourth Amendment protections for cell phone data in other contexts, it is necessary for the courts, Congress, and the Department of Homeland Security to impose limits on searches of electronic devices at the border (which had traditionally been exempt from Fourth Amendment limitations).

3. Please Explain How the Proposed Policy Position Will Address the Issue

This policy will reaffirm the ABA's commitment to personal privacy and the protection of communications and other personal data. By adopting this Resolution, the ABA can assist the work of privacy advocates, lawmakers and litigators that are working to ensure that important Fourth Amendment and privacy law protections are not eroded due to technological changes.

4. Summary of Minority Views or Opposition Internal and/or External to the ABA Which Have Been Identified

The Standing Committee on Law and National Security has reviewed the resolution and opposes it in the current form.