No. 22-1801

UNITED STATES COURT OF APPEALS
FOR THE EIGHTH CIRCUIT

UNITED STATES OF AMERICA,
Plaintiff-Appellee,

v.

HAITAO XIANG,
Defendant-Appellant.

On Appeal from The United States District Court
For The Eastern District of Missouri
Case No. 19-CR-980-HEA-JMB-1
The Honorable Henry E. Autrey, Presiding Judge.

REPLY BRIEF FOR DEFENDANT-APPELLANT HAITAO XIANG

VADIM A. GLOZMAN
MATTHEW P. KRALOVEC
LAW OFFICES OF VADIM A. GLOZMAN
53 W. Jackson Blvd. #1128
Chicago, IL 60604
P: (312)-726-9015
Counsel for Defendant-Appellant Haitao Xiang

TABLE OF CONTENTS

PRELIMINARY STATEMENT 1

ARGUMENT 4

I. The Forensic Search Required a Warrant 4

A. Circuit Courts Have Required Warrants Before Forensically Searching Electronic Devices Seized at the Border 4

B. The Border Search Exception is Limited to Enforcing Customs Laws and Does Not Extend to Investigations Involving the Border 7

C. The Border Search Exception's Limited Purposes Do Not Categorially Exempt Forensic Searches of Electronic Devices 12

D. Any National Security Interest Did Not Justify the Forensic Search 16

E. The Agents Were Not Authorized to Conduct the Search or Investigate Trade Secret Offenses 18

II. There was No Reasonable Suspicion of Current Criminal Activity or that Evidence of a Crime was on the Devices 20

III. The Forensic Search Was Unreasonably Conducted 24

IV. Suppression is Warranted Because the Government Waived Its Good Faith Exception Argument and the Search was Not Specifically Authorized by Precedent 29

CONCLUSION 34

Appellate Case: 22-1801 Page: 2 Date Filed: 09/28/2022 Entry ID: 5202741

TABLE OF AUTHORITIES

CASES

Alasaad v. Mayorkas, 988 F.3d 8 (1st Cir. 2021) 20

Birchfield v. North Dakota, 579 U.S. 438 (2016) 17

Boyd v. United States, 116 U.S. 616 (1886) 8, 9

Carpenter v. United States, 138 S. Ct. 2206 (2018) 13

Carroll v. United States, 267 U.S. 123 (1925) 8

Davis v. Dawson, 33 F.4th 993 (8th Cir. 2022) 9

Davis v. United States, 564 U.S. 229 (2011) 31

Giordenello v. United States, 357 U.S. 480 (1958) 30

Gouled v. United States, 255 U.S. 298 (1921) 10

Kyllo v. United States, 533 U.S. 27 (2001) 13

Puckett v. United States, 556 U.S. 129 (2009) 30

Riley v. California, 573 U.S. 373 (2014) ..... passim

United States v. Aigbekaen, 943 F.3d 713 (4th Cir. 2019) 5, 19, 20

United States v. Alfaro-Moncada, 607 F.3d 720 (11th Cir. 2010) 18

United States v. Barraza-Maldonado, 732 F.3d 865 (8th Cir. 2013) 31

United States v. Bin Laden, 126 F. Supp. 2d 264 (S.D.N.Y. 2000) 17

United States v. Blake, 868 F.3d 960 (11th Cir. 2017) 27

Appellate Case: 22-1801 Page: 3 Date Filed: 09/28/2022 Entry ID: 5202741

United States v. Burston, 806 F.3d 1123 (8th Cir. 2015) 32

United States v. Cano, 934 F.3d 1002 (9th Cir. 2019) ..... passim

United States v. Cotterman, 709 F.3d 952 (9th Cir. 2013) 20

United States v. Dijbo, 151 F. Supp. 3d 297 (E.D.N.Y. 2015) 26

United States v. Falso, 544 F.3d 110 (2nd Cir. 2008) 22

United States v. Hung, 629 F.2d 908 (4th Cir. 1980) 17

United States v. Jones, 565 U.S. 400 (2012) 13

United States v. Kennedy, 427 F.3d 1136 (8th Cir. 2005) 21

United States v. Kim, 103 F. Supp. 3d 32 (D.D.C. 2015) 26

United States v. Kolsuz, 890 F.3d 133 (4th Cir. 2018) 10

United States v. Lara, 815 F.3d 605 (9th Cir. 2016) 32

United States v. LeBron, 729 F.2d 533 (8th Cir. 1984) 26

United States v. Linarez-Delgado, 259 Fed. App'x 506 (3rd Cir. 2007) ... 5

United States v. Lucas, 499 F.3d 769 (8th Cir. 2007) 30

United States v. Manzo-Jurado, 457 F.3d 928 (9th Cir. 2006) 23, 24

United States v. Molina-Isidoro, 884 F.3d 287 (5th Cir. 2018) ..... passim

United States v. Montoya de Hernandez, 473 U.S. 351 (1985) 8

United States v. Morales, 737 F.2d 761 (8th Cir. 1984) 31

United States v. Nee, 261 F.3d 79 (1st Cir. 2001) 30

Appellate Case: 22-1801 Page: 4 Date Filed: 09/28/2022 Entry ID: 5202741

United States v. Ramsey, 431 U.S. 606 (1977) 7, 8, 11, 12

United States v. Raymonda, 780 F.3d 105 (2nd Cir. 2015) 22

United States v. Skaggs, 25 F.4th 494 (7th Cir. 2022) 21

United States v. Stewart, 729 F.3d 517 (6th Cir. 2013) 5

United States v. Tamura, 694 F.2d 591 (9th Cir. 1982) 27

United States v. Touset, 890 F.3d 1227 (11th Cir. 2018) 6, 21

United States v. United States Dist. Court for E. Dist. of Mich., S. Div., 407 U.S. 297 (1972) 17

United States v. Vergara, 884 F.3d 1309 (11th Cir. 2018) 6, 10, 13, 14

United States v. Wanjiku, 919 F.3d 472 (7th Cir. 2019) 4, 7, 24, 30

United States v. Williams, 942 F.3d 1187 (10th Cir. 2019) 4, 21

Warden v. Hayden, 387 U.S. 294 (1967) 10

STATUTES

19 U.S.C. § 1401 18

19 U.S.C. § 1581 18

19 U.S.C. § 1595 19

19 U.S.C. § 1603 19

Act of July 31, 1789, 1 Stat. 29 ..... 7, 8

Act of July 4, 1789, 1 Stat. 24 8

Appellate Case: 22-1801 Page: 5 Date Filed: 09/28/2022 Entry ID: 5202741

OTHER AUTHORITIES

Drew Harwell, *Customs Offices Have Copies Americans' Phone Data at Massive Scale*, The Washington Post, (Sep. 15, 2022)..... 15

Laura K. Donohue, *Customs, Immigration, and Rights: Constitutional Limits on Electronic Border Searches*, 128 Yale L.J.F. 961 (2019)..... 9

Pet. for a Writ of Cert., *United States v. Cano*, No. 20-1043 (Jan. 29, 2021) 14

PRELIMINARY STATEMENT

The government's extraordinary view on border searches expands the narrow warrant exception well past the limits set by the Supreme Court. It seeks near limitless power to search digital devices in any manner it chooses and for any purpose, including investigating general criminal wrongdoing. But the Supreme Court has never sanctioned border searches—or any warrant exception—based on a general interest in investigating. Rather, the Court has only allowed border searches to seize physical goods subject to duties or import restrictions. It has never even allowed customs officers to read the contents of private documents without a warrant, let alone authorize the wholesale search and seizure of a traveler's digital life.

Contrary to the tenor of the government's brief, warrantless border searches of electronic devices are far from being universally accepted by circuit courts. Not only has each circuit addressing this issue reached different results, but half of the circuits have held that a warrant *is* required in the wake of *Riley v. California*, 573 U.S. 373 (2014). The government simply ignores the host of recent Supreme Court cases rejecting the mechanical application of traditional warrant

Appellate Case: 22-1801 Page: 7 Date Filed: 09/28/2022 Entry ID: 5202741

exceptions to new technology. Their stance must be rejected for four main reasons.

First, the government's position extends the border search exception past its traditional justifications. Border searches are reasonable only because customs officers searched for physical goods subject to duties and enforced customs laws. They are not a mechanism for invading travelers' privacy to investigate crimes, as the agents did here. Nor does the government's "national security" interest justify forensic device searches. National security concerns do not even justify all warrantless searches of *actual* security threats. In short, the government offers no valid basis for categorically exempting forensic electronic device searches from the warrant requirement.

Second, the government failed to provide any statute authorizing forensic digital device searches or border searches based on suspected intellectual property offenses. The government attempts to work around this flaw by claiming they can search any device that might be an instrumentality. However, if adopted, this theory turns every criminal offense into a border crime.

Third, despite the government's claims, Monsanto's tip only

Appellate Case: 22-1801 Page: 8 Date Filed: 09/28/2022 Entry ID: 5202741

provided the basis for a contract dispute. The tip only raised suspicions that Dr. Xiang mishandled confidential company information and that he would violate his termination contract. But the law only criminalizes misappropriating trade secret information, not confidential company information. Above all, there was nothing to suggest that *any* type of company information was *ever* transferred to the devices.

Fourth, every aspect of this search was conducted unreasonably. While federal agencies can share information, they are not permitted to exploit a warrant exception in a manner attenuated from the exception's justifications. This unrestrained search violated the agency's directive despite the government's after-the-fact excuses.

At its core, this was not a genuine border search. This Court cannot expand this warrant exception past its narrowly define purposes or mechanically apply the exception to digital devices without sufficiently tethering forensic searches to the exception's purpose. This Court must restore border searches to their permissible scope.

ARGUMENT

I. The Forensic Search Required a Warrant

A. Circuit Courts Have Required Warrants Before Forensically Searching Electronic Devices Seized at the Border

To begin, the government makes incorrect claims about the accepted use of forensic electronic device searches. It argues that circuit courts find that these warrantless searches are permissible border searches, claiming they were not affected by *Riley v. California*, 573 U.S. 373 (2014). *See* Gov't. Br. 27-33. But the government's argument mischaracterizes the caselaw and ignores that at least two circuits have required warrants for these searches.

In fact, most of the government's cases explicitly declined to address the constitutionality of warrantless electronic device searches at all. *See United States v. Molina-Isidoro*, 884 F.3d 287, 290 (5th Cir. 2018) ("We do not decide the Fourth Amendment question" presented by the manual search of a cellphone); *United States v. Wanjiku*, 919 F.3d 472, 479 (7th Cir. 2019) (deciding to "avoid entirely the thorny issue" presented by forensic digital device searches); *United States v. Williams*, 942 F.3d 1187, 1190 (10th Cir. 2019) (declining to determine

the constitutional requirements of forensic digital device searches). And in its two pre-*Riley* cases, one did not involve a digital device like a cellphone or computer, *see United States v. Linarez-Delgado*, 259 Fed. App'x 506, 508 (3rd Cir. 2007) (a videotape), and the other did not contest the actual device search. *See United States v. Stewart*, 729 F.3d 517, 524-26 (6th Cir. 2013) (extended border search challenge).

Moreover, half of the circuits addressing this issue have found that *Riley* has impacted electronic device searches at the border, requiring warrants under certain circumstances. *United States v. Cano*, 934 F.3d 1002, 1019-20 (9th Cir. 2019); *United States v. Aigbekaen*, 943 F.3d 713, 722-23 (4th Cir. 2019). To illustrate, unless CBP agents reasonably believe the devices contain contraband, *Cano* requires a warrant to forensically search them because the government would otherwise have "unfettered access" to "evade the protections laid out in *Riley*[.]" 934 F.3d at 1019-20. In the same way, after considering *Riley*'s balancing test and the privacy interests it announced, *Aigbekaen* found "it would be patently unreasonable to permit highly intrusive forensic" searches without a warrant if the search did not further a border interest. 943 F.3d at 722-23.

While the government claims, "it is telling that no post-*Riley* decision has required a warrant for a border search of an electronic device," Gov't. Br. 32-33 (citing *Molina-Isidoro*, 884 F.3d at 292), it is even more telling that, after this pronouncement, two circuits *have* required warrants based on *Riley*. Even judges in the Eleventh Circuit cases, where both panels split 2-1, expressed concerns about the government's position, stating it has never been accepted "by the Supreme Court or … any appellate court." *United States v. Touset*, 890 F.3d 1227, 1238-39 (11th Cir. 2018) (Corrigan, J., concurring in part and in judgment); *see also United States v. Vergara*, 884 F.3d 1309, 1314-19 (11th Cir. 2018) (J. Pryor, J., dissenting) (explaining that, after *Riley*, the answer to forensic electronic device searches "is accordingly simple—get a warrant."). Courts have recognized that the Fourth Amendment landscape has changed since *Riley*. This Court should do the same.

Appellate Case: 22-1801 Page: 12 Date Filed: 09/28/2022 Entry ID: 5202741

B. The Border Search Exception is Limited to Enforcing Customs Laws and Does Not Extend to Investigations Involving the Border

Since its inception, the border search exception has been a *narrow* exception based on grants of authority by the First Congress. The Supreme Court has linked this "congressionally-granted, search-and-seizure authority to two main purposes: to allow the regulation of the collection of duties, and to prevent the introduction of contraband into this country." *Wanjiku*, 919 F.3d at 480. The government argues that this limited exception permits searches for evidence of any "cross-border" crime, even if the only border aspect of such crime is traveling with the device. Gov't. Br. 34-38. Yet, the Supreme Court has never permitted border searches on these grounds or even allowed customs officers to read the content of personal material without a warrant. *See United States v. Ramsey*, 431 U.S. 606, 624 n.18 (1977).

The foundation of the border search exception is premised on an early customs statute that allowed customs officers "to enter any ship or vessel, in which they shall have reason to suspect any goods, wares or merchandise subject to duty shall be concealed," and seize those items without a warrant. Act of July 31, 1789, § 24, 1 Stat. 29, 43; *see also*

United States v. Montoya de Hernandez, 473 U.S. 351, 537 (1985). The Supreme Court reasoned that "warrantless border searches are not 'unreasonable' within the meaning of the Constitution" because the same Congress that enacted this statute also proposed the Fourth Amendment. *Molina-Isidoro*, 884 F.3d at 295 (Costa, J., specially concurring); *see also Boyd v. United States*, 116 U.S. 616, 623-24 (1886); *Ramsey*, 431 U.S. at 617; *Carroll v. United States*, 267 U.S. 123, 150-51 (1925). In this way, border searches have always been limited by what the First Congress believed was reasonable. And they did not believe it was reasonable for customs officers to search private material for things unrelated to collecting duties and import restrictions.

The early customs statutes differentiated between impersonal, physical goods and personal, private papers. The statute permitted warrantless seizures of only "goods, wares or merchandise," not personal papers and documents like the type contained in digital devices' data. Act of July 31, 1789, § 24, 1 Stat. at 43. An accompanying statute specifying the "goods, wares and merchandise" subject to import laws included no written documents among the items listed. *See* Act of July 4, 1789, § 1, 1 Stat. 24. These early statutes—the basis for the

Appellate Case: 22-1801 Page: 14 Date Filed: 09/28/2022 Entry ID: 5202741

border search exception—establish that Congress was concerned with "the failure to pay duties at the border" and the "movement of uncustomed goods." Laura K. Donohue, *Customs, Immigration, and Rights: Constitutional Limits on Electronic Border Searches*, 128 Yale L.J.F. 961, 973-77 (2019).

The Founders chose to exclude searches through private material for a reason: the warrantless search and seizure of private papers drove them to Revolution. *Davis v. Dawson*, 33 F.4th 993, 1002-05 (8th Cir. 2022) (Stras, J., concurring) (describing how *Entick*'s case, where officers warrantlessly seized his private "papers," was one of the cases that "inspired the Revolution[.]"); *see also Boyd*, 116 U.S. at 626 (calling *Entick* a "landmark[] of English liberty" that was "applauded by the lovers of liberty in the colonies."). For this reason, the Supreme Court struck down a Civil War statute that allowed customs officers to search private material: the government could seek items "liable to duties" because those efforts were "totally different things from a search for and seizure of a man's private books and papers for the purpose of obtaining information therein contained." *Boyd*, 116 U.S. at 623-24.

In this manner, the border search exception has always been

Appellate Case: 22-1801 Page: 15 Date Filed: 09/28/2022 Entry ID: 5202741

premised on enforcing duties and customs laws—not investigating crimes, "cross-border" or otherwise. *Cano*, 934 F.3d at 1013 (explaining that border searches are "not for general law enforcement purposes."); *United States v. Kolsuz*, 890 F.3d 133, 143 (4th Cir. 2018); *Vergara*, 884 F.3d at 1317 (J. Pryor, J., dissenting). To the First Congress, searching and seizing impersonal objects subject to duties was reasonable, but rummaging through private material was not. And this makes sense. Customs officers enforce customs laws, not investigate crimes.

This traditional premise still limits the scope of border searches. *See Molina-Isidoro*, 884 F.3d at 295 (Costa, J., specially concurring) (explaining that even modern customs statutes are "also limited to" the "actual objects[.]"). The government claims that *Boyd*'s premise no longer applies because the later formulated "mere evidence rule" has been denounced. *See* Gov't. Br. 34-35. This is wrong. The "mere evidence rule" was announced in *Gouled v. United States*, which broadened *Boyd*'s holding to all searches and seizures of all private property. 255 U.S. 298, 306-13 (1921). It did not involve a border search. *Id*. More broadly, *Warden v. Hayden*, 387 U.S. 294 (1967), is generally accepted as rejecting a property interest view of the Fourth Amendment that

required the government to have a superior property interest before seizing objects. *See*, *e.g.*, *Molina-Isidoro*, 884 F.3d at 296 n.7 (Costa, J., specially concurring).

What is more, since *Hayden*, the Supreme Court has continuously relied on *Boyd* for the premise that border searches are constitutionally reasonable. *Id.*; *see also Ramsey*, 431 U.S. at 617 (stating *Boyd*'s "interpretation" of the border search exception "had been faithfully adhered to by this court."). *Gouled* transformed *Boyd*'s Fourth Amendment holding into something beyond border searches. However, *Boyd*'s core premise, that the First Congress's view of reasonableness limits the border search exception, still rings true. *See id.* (explaining that "The First Congress authorized customs officials to search for and seize 'goods, wares, and merchandise" concealed "to avoid duties," "it did not provide that authority to obtain evidence of crimes other than the contraband itself.").

The Supreme Court even indicated that this traditional physical object limitation still applies. For example, when it found that it was reasonable to open international mail to search for drugs, it repeatedly stressed that the officers were prohibited by statute from reading the

private contents of the mail. *Ramsey*, 431 U.S. at 618-25. It specifically reserved judgment on whether the "full panoply of Fourth Amendment requirements" would be needed "in the absence of regulatory restrictions." *Id.* at 624 n.18.

C. The Border Search Exception's Limited Purposes Do Not Categorially Exempt Forensic Searches of Electronic Devices

The government cannot meaningfully contest that travelers have an immense privacy interest in their devices, which contain more private information than any type of property. *See* Gov't. Br. 28-33. Nor can it contest that forensic searches are invasive intrusions. Instead, the government argues that this Court should ignore *Riley*'s constitutional principles and categorically exempt forensic searches because digital devices are property. *Id.*

But this ignores the core premise of *Riley*: digital devices are *fundamentally* different. *Riley*, 573 U.S. at 391-95. Despite the government's insistence, electronic devices are not the same as property traditionally crossing the border. As the Supreme Court has repeatedly made clear, pre-digital age warrant exceptions—here, border searches of impersonal objects—cannot be mechanically applied to digital age

Appellate Case: 22-1801 Page: 18 Date Filed: 09/28/2022 Entry ID: 5202741

searches. *Id.*; *see also Carpenter v. United States*, 138 S. Ct. 2206, 2214 (2018); *United States v. Jones*, 565 U.S. 400 (2012); *Kyllo v. United States*, 533 U.S. 27, 34 (2001). Yet, this is exactly what the government seeks.

Despite the wide-ranging power the government claims for conducting border searches—which far exceeds the traditional justifications—it fails to explain how warrantless forensic searches substantially advance those interests. For example, forensic searches do not meaningfully further the detection-of-contraband interest—the traditional rationale—because electronic devices "do not contain the physical contraband that border searches traditionally have prevented from crossing the border." *Vergara*, 884 F.3d at 1317 (J. Pryor, J., dissenting); *accord Molina-Isidoro*, 884 F.3d at 295 (Costa, J., concurring). Just as physical weapons cannot be hidden in digital data, physical contraband cannot be hidden in digital data.

To counter, the government claims it can conduct the searches to detect "digital contraband" and takes an absurdly expansive view of what that encompasses. Gov't. Br. 31-35. Specifically, it argues that digital contraband includes child pornography and digital evidence of

any crime.[1] Notably, the government has argued in other cases that digital contraband was "limited almost exclusively to child pornography." Pet. for a Writ of Cert., 26, *United States v. Cano*, No. 20-1043 (Jan. 29, 2021); *see also Cano*, 934 F.3d at 1021 n.13 ("the detection-of-contraband justification would rarely seem to apply … outside the context of child pornography."). Even assuming, *arguendo*, that digital evidence qualifies as digital contraband, there is no support for the contention "that the ability to conduct a warrantless search would make much of a difference" in preventing digital evidence from crossing the border. *Riley*, 573 U.S. at 390; *see also Vergara*, 884 F.3d at 1317 (J., Pryor, J., dissenting) (explaining that "unlike physical contraband, electronic contraband is borderless" due to the internet).

To tether the warrantless search to the exception, the search must address a "prevalent" problem and substantially further its purpose. *Id.* In *Riley*, it was plausible that the phone searches could reveal evidence

---

[1] At various points, the government claims that CBP can search any device that was used as an instrumentality or contains evidence of a crime because the devices are crossing the border "contrary to the laws of the United States." *See* Gov't. Br. 38. As discussed below, this irrational argument improperly exceeds both the border search exception and Congress's intended limits.

encountered in traditional searches, which would further the exception's rationale. *Id*. at 399-401. Still, this could not justify the massive privacy invasion. The possibility of finding, for example, a particular bank statement "did not justify a search of every bank statement from the last five years." *Id*. at 400. "[T]he fact that a search in the pre-digital era could have turned up a photograph or two" of illicit material, "does not justify a search of thousands of photos in a digital gallery." *Id*.

CBP officials recently revealed that they are using these invasive searches for general law enforcement purposes, not detecting digital contraband.[2] After forensically searching cellphones and computers, CBP agents upload the seized data, including messages and call details, to a central database that thousands of officers can subsequently search. *Id*. This creates wide-ranging and dangerous invasions of privacy. There is no justification for categorially exempting electronic devices to give CBP agents this kind of unfettered power.

---

[2] Drew Harwell, *Customs Offices Have Copies Americans' Phone Data at Massive Scale*, The Washington Post, (Sep. 15, 2022) https://www.washingtonpost.com/technology/2022/09/15/government-surveillance-database-dhs/

D. Any National Security Interest Did Not Justify the Forensic Search

The government claims the forensic search was justified based on its interest in investigating national security concerns—again, outside the traditional rationale. Gov't. Br. 28-32. To be clear, at the time of the search, SA Depke and TFO Beck did not have any evidence at the time to establish that this was a national security matter. Tr. 67-68. Before they searched his devices, they had no information linking Dr. Xiang to any Chinese government agent or entity. Tr. 43, 68-69. Monsanto did not even know whether or not Dr. Xiang was authorized or not to send anything to NERCITA. Tr. 8-9, 53-54; R. Doc. 114-1, p.1. Though he had access to trade secrets during his employment, there was no evidence that the information underlying Monsanto's suspicions constituted trade secrets. Tr. 54-55.

Regardless, the government is still constrained when it acts on national security concerns. Without a FISA warrant, the Fourth Amendment prevents the government from conducting warrantless searches based on national security matters unless the target is an agent of a foreign power, and the search is "conducted primarily for foreign intelligence purposes." *United States v. Bin Laden*, 126 F. Supp.

2d 264, 277 (S.D.N.Y. 2000) (citing *United States v. Hung*, 629 F.2d 908, 915-18 (4th Cir. 1980)). "If foreign intelligence collection is merely *a* purpose and not the *primary purpose* of a search, the [foreign intelligence] exception does not apply." *Id.* at 278 (emphasis original). Even when acting on national security matters, the government is not given carte blanche search authority. *United States v. United States Dist. Court for E. Dist. of Mich., S. Div.,* 407 U.S. 297, 316-17 (1972). The national security interest does not even justify the search conducted here, let alone the categorical exemption of digital devices.

Nor would a warrant interfere with the government's ability to protect the border. Repeatedly, the law has rejected this argument as a basis for carving out a warrant exception, especially as new technologies allow officers to obtain warrants within minutes. *See Birchfield v. North Dakota*, 579 U.S. 438, 487-91 (2016); *Cano*, 934 at 1020. In the case of an actual national security threat, like potential terrorist attacks. In that case, CBP agents could still warrantlessly search under the exigent circumstances exception. They could otherwise seize the devices if they had probable cause—absent here—and retain them until they obtained a warrant.

E. The Agents Were Not Authorized to Conduct the Search or Investigate Trade Secret Offenses

CBP agents can only conduct border searches when authorized by Congress. *See*, *e.g.*, *United States v. Alfaro-Moncada*, 607 F.3d 720, 726 (11th Cir. 2010). Yet, despite this simple requirement, the government has failed to provide any authorizing statute. Gov't. Br. 38-39. For example, the government claims that one statute allows CBP to search "any trunk, package, or cargo," claiming this statute applies to air travel. *Id*. (citing 19 U.S.C. § 1581 "Boarding Vessels"). Yet, § 1581 is limited to a "vessel or vehicle," which explicitly excludes air travel. *See* 19 U.S.C. § 1401(a)-(b) (stating that vessels and vehicles do "not include aircraft.").

On this point, the government's main argument rests on the mistaken premise that devices containing evidence of any crime violate customs laws. Gov't. Br. 34-39. In essence, it claims the devices themselves constitute "merchandise," and they were crossing the border "contrary to the laws of the United States" because they possibly contained evidence. *Id*. Such interpretation transforms every crime into a border offense merely because a traveler has electronic evidence on his device and takes it abroad. "If the border search exception is to

retain any distinction from the government's generalized interest in law enforcement and combatting crime, it cannot be invoked to sanction invasive and nonroutine warrantless searches of all suspected" criminals "nor the suspected 'instrumentalities' of their" crimes. *Aigbekaen*, 943 F.3d at 724.

Nor did Congress intend this reach. For instance, Congress authorized CBP agents to apply for search and seizure warrants. *See* 19 U.S.C. § 1595. When property "violat[es] the customs laws," but is not subject to search under § 1595—the statute cited by the government—CBP agents may seize the items "in the same manner as provided by a search warrant[.]" 19 U.S.C. § 1603. If CBP agents were permitted to seize digital devices merely because they were instrumentalities or contained evidence, these statutes would be meaningless. *Cf. Cano*, 934 F.3d at 1017 (explaining digital evidence is "not contraband, and there is no law prohibiting the importation of mere evidence of a crime."). Any piece of property crossing the border that violated any law would satisfy the government's standard.

In the end, the government failed to provide any statute authorizing forensic searches of digital devices or empowering the CBP

to enforce intellectual property offenses. Because none exist.

II. There was No Reasonable Suspicion of Current Criminal Activity or that Evidence of a Crime was on the Devices

Most circuits addressing border searches agree that, at a minimum, agents need reasonable suspicion. *See*, *e.g.*, Br. 42-43; *Aigbekaen*, 943 F.3d at 720-23. While the government attempts to downplay the invasion by calling it a "limited key-word search," Gov't. Br. 42, it ignores that the keyword search came after Dr. Xiang's devices were forensically imaged using specialized software. Tr. 37-38. Each keyword searched the entire contents of the digital devices. *United States v. Cotterman*, 709 F.3d 952, 966 (9th Cir. 2013) (describing this type of forensic exam as "a computer strip search."). Even the CBP considers this an advanced search requiring reasonable suspicion. *Alasaad v. Mayorkas*, 988 F.3d 8, 13-14 (1st Cir. 2021).

Together, all the information the agents knew barely added up to a company violation. This is a far cry from criminal wrongdoing. The government takes issue with the fact that SA Depke was essentially investigating a contract dispute. Gov't. Br. 36. Yet, that is all it was. Monsanto was suspicious that Dr. Xiang was mishandling, or at worst misappropriating, *company information*. Tr. 54-55, 71. Monsanto

Appellate Case: 22-1801 Page: 26 Date Filed: 09/28/2022 Entry ID: 5202741

pointed to Dr. Xiang's behavior when he signed the termination contract, which covered all *company information*, and to his Google searches and emails to support this belief. Tr. 25-27. The government ignores the fundamental problem. *Company information* is not the same thing as *trade secret information*. The distinction is essential. Misappropriating trade secret information is a crime. Misappropriating general company information or failing to follow company email protocols is a simple contract dispute.[3]

Even when considering the old Google searches, the government fails to suggest (1) current criminal wrongdoing; or (2) any reason for believing that evidence such would be located on the specific devices. *See*, *e.g.*, *United States v. Kennedy*, 427 F.3d 1136, 114 (8th Cir. 2005). The government uses later learned facts to insert artificial significance

---

[3] For this reason, the government's cases miss the mark because they all present suspicion of criminal offenses. *See*, *e.g.*, *Touset*, 890 F.3d at 1238 (defendant made payments to a Western Union account that agents knew was associated with an email account containing child pornography); *United States v. Skaggs*, 25 F.4th 494, 500 (7th Cir. 2022) (defendant was a director of an organization that had the name of a well-known child pornography site); *Williams*, 942 F.3d at 1189-91 (defendant's travel tracked a string of terrorist attacks and he lied about visiting countries to which he was barred from traveling).

into these searches, claiming that this slow-moving "plot," beginning with a job interview in 2015, meant that Dr. Xiang was committing a crime years later. Gov't. Br. 47-48. However, the searching agents did not know about this interview. They learned all of this from searching his devices. Tr. 43, 72-73; R. Doc. 99, p.9. Hence, this information is incapable of legitimizing searches done prior to its obtainment. The Google searches concerned accusations of merely providing company information to third parties. This suggests civil liability rather than criminal.

Nonetheless, these Google searches do not indicate that any evidence of a crime would be found on Dr. Xiang's devices a year later. SA Depke admitted there was no evidence any company information was ever transferred to them. Tr. 73-76. Even when past internet activity suggests criminal activity, it does not establish that evidence will be found on the computer months later when nothing suggests anything was transferred to the devices. *United States v. Raymonda*, 780 F.3d 105, 115-17 (2nd Cir. 2015); *see also United States v. Falso*, 544 F.3d 110, 117 (2nd Cir. 2008) (holding computer search was not justified on the mere fact the defendant tried to access an illicit

Appellate Case: 22-1801 Page: 28 Date Filed: 09/28/2022 Entry ID: 5202741

website).[4]

Although the agents need not rule out every possible innocent explanation, "the totality of circumstance" requires them to weigh factors "for and against reasonable suspicion." *United States v. Manzo-Jurado*, 457 F.3d 928, 938 (9th Cir. 2006). Taken together, the agents lacked objective facts that Dr. Xiang was engaged in current criminal activity. The difference between (1) evidence of providing confidential information to third parties; and (2) evidence of providing trade secrets to third parties is the difference between evidence indicting criminal activity and evidence indicating none.

The agents' beliefs at the time of the search failed to establish that the information they possessed supported criminal wrongdoing. The surrounding circumstances (like improper emails, potentially authorized transmission to NERCITA, travel to China, and nervous behavior observed by a biased source) do not provide insight into this

---

[4] It does not matter that *Raymonda* dealt with probable cause as opposed to reasonable suspicion because, under either standard, the facts must still establish that the specific devices contained contraband or evidence. Br. 44. The reasonable suspicion standard does not eliminate this requirement.

flaw. *Id.* at 937 (stating "ambiguous" observations and traits common to both legal and illegal activity "does little to arouse reasonable suspicion.").[5] Above all, *none* of the information possessed by the searching agents indicated that anything was ever transferred to the devices. Accordingly, there was no reasonable suspicion to support this nonroutine search.

III. The Forensic Search Was Unreasonably Conducted

Every aspect of this search smacks of unreasonableness. Neither this Court nor the Supreme Court has ever sanctioned a border search that was this invasive and attenuated from the underlying purposes that legitimate border searches. Yet, the government contorts the record to paint this search as just a typical border search. It was not.

First, the agents exploited the border search exception so that the FBI and SA Depke could forensically search the devices for their own

---

[5] Despite the government's claims, this Court has repeatedly held that circumstances applicable to a large portion of innocent persons add little—if any—insight to reasonable suspicion. Br. 44-50. This is especially true regarding Dr. Xiang's trip to China because it was his birth country. *Compare Wanjiku*, 919 F.3d at 487 (finding trip added to suspicion because the defendant "had no obvious connection" to a country known for sex tourism).

investigation. Dr. Xiang does not contest that federal agencies can share and rely on information between each other in certain situations. Gov't. Br. 51. But that is not the full story here. The government omits that the entire purpose of this search was to further SA Depke's investigation. CBP has no actual interest or need for assistance. After SA Depke approached TFO Beck about Dr. Xiang, TFO Beck asked if *he* wanted CBP to seize the devices and send them to *him* for *his* investigation. Tr. 49-52, 60-61, 79, 90. The devices were immediately sent to the FBI's St. Louis office without any attempt to search them. Tr. 58, 112-13. After the seizure, SA Depke thanked the CBP "for their assistance" in his investigation. Tr. 60-61, 79, 90. Though the CBP may have decided to seize the devices, it was always for SA Depke, not for any border-related investigation concern to CBP. They never even bothered to get the results of the search. Tr. 80-81.

Border searches conducted to further a pre-existing investigation into general wrongdoing are unreasonable because they are too attenuated from the exception's core purpose. For example, in *United States v. Kim*, a forensic search of a laptop was unreasonable because another agency directed CBP agents seize the device so they could

Appellate Case: 22-1801 Page: 31 Date Filed: 09/28/2022 Entry ID: 5202741

search it for evidence relating to a pre-existing investigation. 103 F. Supp. 3d 32, 59 (D.D.C. 2015). The search was too disconnected from proper border-search authority. *Id.*; *see also Molina-Isidoro*, 884 F.3d at 289 n.1 (describing the search in *Kim* as "not like the typical border-search[.]"). In *United States v. Dijbo*, a forensic "sneak peek" search was unreasonable when CBP agents searched the defendant's cellphone for evidence as part of their pre-existing investigation into a narcotics importation conspiracy. 151 F. Supp. 3d 297, 299-306 (E.D.N.Y. 2015). The CBP agent was not looking for genuine contraband but was attempting to "expand the definition of a border search." *Id.* at 309. Just as they did here, the agents "sought to sidestep [the] constitutional guarantees." *Id.* at 310.

Second, the forensic search was unreasonably intrusive. The FBI indiscriminately searched and seized the devices' entire contents when they created the forensic images. The search and seizure was akin to overbroad search warrants that allow officers to conduct impermissible rummages. *See United States v. LeBron*, 729 F.2d 533, 536-39 (8th Cir. 1984) (suppressing evidence based on an overbroad warrant for documents relating to "stolen property" because it did not provide a way

Appellate Case: 22-1801 Page: 32 Date Filed: 09/28/2022 Entry ID: 5202741

to distinguish between non-stolen and stolen property, allowing an indiscriminate rummage); *United States v. Blake*, 868 F.3d 960, 974 (11th Cir. 2017) (finding Facebook search warrants that required disclosure "of virtually every kind of data" fatally overbroad because the warrant should have limited the data to specific periods when the defendant was a conspiracy member). This wholesale seizure of digital data for "later detailed examination" is "the kind of investigatory dragnet that the Fourth Amendment was designed to prevent." *United States v. Tamura*, 694 F.2d 591, 595 (9th Cir. 1982).

Third, the agents violated CBP's directive, further indicating that the forensic search was unreasonable as the agents themselves did not treat this as a true border search. To be clear, Dr. Xiang does not argue the evidence must be suppressed for violating the directive alone. Gov't. Br. 62. Instead, the agents' failure to follow the directive illustrates the fact that this search was unreasonable because they did not even confine their search to their own rules. Br 53-55.

To this end, the government attempts to use after-the-fact explanations that do not withstand the record. For instance, it claims that the devices could be shipped to the FBI for subject matter

assistance. Gov't. Br. 54. Yet, it is undisputed that CBP agents made no attempts to search the devices before shipping them to St. Louis. They did nothing to indicate they were in need of FBI assistance. Tr. 46, 58, 112-14. The directive requires that the CBP agents must first encounter the material before seeking subject matter assistance. Br. 54. Hence, the agents purportedly *guessed* that they would encounter such material. Tr. 73-75. Furthermore, the agents needed supervisor approval before sending the devices to an outside agency or extending the search past the allotted timeframe. But SA Depke did not even know they needed such approval. Tr. 64. Though TFO Beck recalled that he might have gotten approval for the initial extension. Tr. 118. He did not obtain them.[6]

Indeed, the record reveals that the agents were not acting on these concerns when the search occurred. The Inspection Results does not list any need for assistance, stating only that the devices were detained "at the request of CBP/FBI JTTF St. Louis[.]" The government

---

[6] Contrary to the government's claims, Gov't. Br. 10-12, Monsanto did not confirm the seized documents were considered trade secrets until at least 17 days after the devices were seized. Tr. 37, 44. And SA Depke kept the devices for another month before getting a warrant.

did not produce any email or document showing supervisor approval. In fact, both agents repeatedly distanced themselves from the seizure, claiming they were not communicating with the seizing agents or that they did not know why they took certain actions. Thus, these excuses were nothing more than after-the-fact attempts to explain their failure to follow the policy. SA Depke's email reveals why the devices were sent to St. Louis: he wanted to search them.

Simply put, this was never a border search, especially not a reasonable one. The forensic search was invasive and indiscriminately seized all of Dr. Xiang's data, regardless of whether it related to "digital contraband." SA Depke admitted he wanted to search the devices but lacked the authority to do so. The subsequent attempts to sidestep the Fourth Amendment were not reasonable.

IV. Suppression is Warranted Because the Government Waived Its Good Faith Exception Argument and The Search Was Not Specifically Authorized by Precedent

For the first time, the government argues that the evidence obtained from the forensic search should not be suppressed because the agents were acting in good faith reliance that the search was authorized. Gov't. Br. 62-64. Despite always being available, the

Appellate Case: 22-1801 Page: 35 Date Filed: 09/28/2022 Entry ID: 5202741

government has never raised the argument until now, and the district court and magistrate did not address it. Therefore, the government waived the argument. *See Puckett v. United States*, 556 U.S. 129, 138 (2009) (explaining that an argument is waived when "intentionally relinquished or abandoned").

Indeed, the government is "barred from raising Fourth Amendment arguments for the first time on appeal." *United States v. Lucas*, 499 F.3d 769, 784 (8th Cir. 2007) (Bye, J., dissenting in part); *see also Steagald v. United States*, 451 U.S. 204, 208-11 (1981) (finding that the government waived its right to argue that the defendant lacked standing to challenge a search); *Giordenello v. United States*, 357 U.S. 480, 487 (1958) (finding that the government could not argue a new basis for upholding an arrest for the first time on appeal); *United States v. Nee*, 261 F.3d 79, 86 (1st Cir. 2001) (holding that the government waived its argument regarding probable cause). Even in *Wanjiku*—the government's cited case for this issue—the Seventh Circuit stated the government would have waived the good faith argument had the defendant argued, as Dr. Xiang does here, that the search required a warrant. 919 F.3d at 486-87. By failing to raise the argument before,

"the government has lost its right to" argue that evidence should not be suppressed for good-faith reliance. *United States v. Morales*, 737 F.2d 761, 763 (8th Cir. 1984).

Even if this Court addresses the government's new argument, the good-faith exception does not apply. Foremost, the agents cannot rely on Seventh Circuit precedent. Gov't. Br. 63-64. While the devices were seized at O'Hare, they were forensically searched in St. Louis. Tr. 30-32, 37. For the good faith exception to apply, the agents must "strictly comply with binding appellate precedent governing the jurisdiction *in which they are acting*." *United States v. Barraza-Maldonado*, 732 F.3d 865, 687 (8th Cir. 2013) (emphasis added). Unlike the officers in *Barraza-Maldonado*, the agents here acted in the Eighth Circuit when they searched the devices. *Id.* at 867-69.

Regardless, no binding precedent specifically authorized the forensic search of Dr. Xiang's electronic devices. *Davis v. United States*, 564 U.S. 229, 241 (2011) (requiring that the "binding appellate precedent *specifically authorizes* a particular police practice[.]") (emphasis original). The government has not cited any Supreme Court or Eighth Circuit case—because none exist—specifically authorizing

warrantless forensic border searches of digital devices. Gov't. Br. 62-63. Nor has it cited any binding precedent that permits sending the devices to another agency to in support of that agency's pre-existing investigation. Instead, the government vaguely argues that the Supreme Court has allowed warrantless border searches of property, so the agents believed they could search digital data without limits.

The good faith exception does not apply when the government attempts to expand the scope of authorized searches. *See*, *e.g.*, *United States v. Lara*, 815 F.3d 605, 614 (9th Cir. 2016) (holding that the good faith exception did not apply when it was "plausibly" arguable that precedent authorized the police practice). For example, the government could not use the exception when police conducted an unlawful drug-dog sniff of an apartment window even though precedent allowed dog sniffs of an apartment door. *United States v. Burston*, 806 F.3d 1123, 1128-29 (8th Cir. 2015). The precedent did not "specifically authorize" a dog sniff in this manner, and the cases did not "present similar facts[.]" *Id.* at 1129. In *Cano*, the Ninth Circuit had recently permitted a border search of a digital device for child pornography. 934 F.3d at 1021-22. Still, the good faith exception did not apply because the precedent did not

specifically authorize a search for mere evidence. *Id*.

For this reason, the good faith exception cannot be applied here. While the Supreme Court and Eighth Circuit have permitted border searches, it is a leap too far to say that this "specifically authorized" CBP agents to forensically search digital devices, particularly in the manner done here. Moreover, the government has not presented *any* binding precedent that is remotely similar.

CONCLUSION

WHEREFORE, Defendant-Appellant Haitao Xiang respectfully requests that this Court vacate his convictions, remand for further proceedings, and any other just and equitable relief deemed necessary and appropriate by the Court.

Respectfully Submitted,

/s Vadim A. Glozman
Counsel for Haitao Xiang
VADIM A. GLOZMAN
LAW OFFICES OF VADIM A. GLOZMAN
53 W. Jackson Blvd. Suite, 1128
Chicago, IL 60604
P: 312-726-9015

/s Matthew P. Kralovec
Counsel for Haitao Xiang
MATTHEW P. KRALOVEC
LAW OFFICES OF VADIM A. GLOZMAN
53 W. Jackson Blvd. Suite, 1128
Chicago, IL 60604
P: 312-726-9015

RULE 32 CERTIFICATE OF COMPLIANCE

This reply brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this reply brief contains 6,313 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(iii).

This brief complies with the typeface and style requirements of Fed. R. App. P. 32(a) because this brief has been prepared in a proportionally spaced typeface using 14-point Century Schoolbook in Microsoft Word for Windows 365.

In accordance with 8th Cir. R. 28A(h)(2), this brief has been scanned for viruses and are virus free.

Respectfully Submitted,

/s Vadim A. Glozman
Counsel for Haitao Xiang
VADIM A. GLOZMAN
LAW OFFICES OF VADIM A. GLOZMAN
53 W. Jackson Blvd. Suite, 1128
Chicago, IL 60604
P: 312-726-9015

/s Matthew P. Kralovec
Counsel for Haitao Xiang
MATTHEW P. KRALOVEC
LAW OFFICES OF VADIM A. GLOZMAN
53 W. Jackson Blvd. Suite, 1128
Chicago, IL 60604
P: 312-726-9015

CERTIFICATE OF SERVICE

I, Vadim A. Glozman, hereby certify that I caused a true and accurate copy of the attached Reply Brief for Defendant-Appellant Haitao Xiang to be served upon the government by electronically serving it through the CM/ECF system on September 28, 2022.

Respectfully Submitted,

Dated: Sept. 28, 2022.

/s Vadim A. Glozman
Counsel for Haitao Xiang
VADIM A. GLOZMAN
LAW OFFICES OF VADIM A. GLOZMAN
53 W. Jackson Blvd. Suite, 1128
Chicago, IL 60604
P: 312-726-9015