Prepare For More Electronic Device Searches At U.S. Borders

By George Varghese, Benjamin Conery and Sierra Shear (December 15, 2020)

George Varghese

Benjamin Conery

Sierra Shear

In recent years, the U.S. Department of Justice has brought an increasing number of cases aimed at combating economic espionage as part of its China Initiative.[1] This effort has included cases against scientific researchers working at American universities for alleged failures to disclose foreign ties or funding, and against efforts to smuggle federally funded research to China.

While federal prosecutors have charged a number of academic researchers across the U.S. with a variety of crimes, many of these cases have one thing in common: The charges stem from a search of the researcher's physical luggage or electronic devices at an airport.

For instance, in January the government charged Yanqing Ye, a lieutenant of the China's People's Liberation Army and member of the Chinese Communist Party, with falsely identifying herself as a student at Boston University, and lying on a visa application about her ongoing military service.

In fact, prosecutors allege that Ye continued to work for the PLA in the U.S., conducting research, assessing U.S. military websites, and sending documents and information to China. The charges followed an interview of Ye at Boston's Logan International Airport and a search of her electronic devices that revealed extensive communications between Ye and a PLA officer, including specific taskings.

That same day, prosecutors announced charges against Zaosong Zheng, a cancer researcher at Beth Israel Deaconess Medical Center in Boston, for allegedly stealing 21 vials of biological research and attempting to smuggle them out of the U.S. federal officers at Logan Airport allegedly discovered the vials hidden in a sock in Zheng's luggage as he was attempting to fly to China.

In June, Xin Wang, a scientific researcher at the University of California, San Francisco, was arrested at Los Angeles International Airport for visa fraud. According to the government, Wang was interviewed by federal agents as he was preparing to depart the country for China. During the interview, Wang stated that he was a PLA officer and was carrying some of his UCSF research work with him back to China to share with PLA researchers.

These cases are just a few examples of recent China Initiative cases brought by the DOJ based largely on the evidence discovered during airport border searches. The number of these cases has been on the rise. U.S. Attorney Andrew Lelling has referred to the cases announced so far as only the tip of the iceberg. Assistant Attorney General for National Security John Demers has explained:

> [T]he Justice Department will continue to prioritize investigations like these, to ensure that China understands that this criminal conduct is not an acceptable business or economic development practice.

And as the DOJ does so, border searches, conducted by U.S. Customs and Border Protection and U.S. Immigration and Customs Enforcement, will remain one of its most essential investigative tools.

But while the three cases identified above represent successful border searches where evidence was actually found, there are countless more where innocent travelers have been questioned, and devices seized and examined without results.

Academic researchers and visiting students have described being targeted by CBP agents, aggressively questioned, and having their devices taken from them. Often, these encounters have led to missed flights, and months without laptops or cellphones and the critical information contained on them.

This article describes the current state of the law related to border searches. In particular, this article will focus on the law as it pertains to CBP and ICE authority to seize and examine electronic devices, and recent legal challenges to that authority that could ultimately change the landscape for these searches.

We conclude with practical advice for educational institutions, companies, and other organizations to help their researchers, students and employees prepare to travel to and from the U.S.

The Current State of the Law

Although the U.S. Constitution prohibits warrantless searches under most circumstances, the U.S. Supreme Court has long recognized a border search exception that allows broader latitude in protecting the integrity of the border.[2]

The government has a "paramount interest in maintaining 'territorial integrity' at the border" in order to regulate trade, protect national security, and prevent illegal smuggling of people and contraband.[3] Accordingly, "individuals have a reduced expectation of privacy at the international border," which includes airports.[4]

While there is some uncertainty as to the permissible scope of warrantless searches at the border, "the border search exception is not limitless."[5] Courts have construed this exception to permit the search of a person, their checked and carry-on luggage[6] and — perhaps most notably — electronic devices for all individuals, including U.S. citizens.

For their parts, CBP and ICE each have adopted policies distinguishing between basic searches and advanced border searches.[7] Basic searches, which each agency defines as "any border search that is not an advanced search," do not require any suspicion.[8] Typically, that involves a manual review of a phone or laptop where an agent scrolls through the unlocked device, looking for contraband.

On the other hand, advanced searches are defined as:

> any search in which an officer connects external equipment, through a wired or wireless connection, to an electronic device, not merely to gain access to the device, but to review, copy and/or analyze its contents.[9]

Advanced searches typically involve the seizure of the electronic device and a forensic review, usually done off-site.

Under both the CBP and ICE policies, advanced searches require reasonable suspicion that contraband will be located on the device. The reasonable suspicion standard is the same that is required for a Terry stop or stop-and-frisk search,[10] and less than the probable cause required for a warrant under the Fourth Amendment.

Developments in the Law

Amid increased border searches involving electronic devices,[11] in September 2017, in Alasaad v. Nielsen, 11 plaintiffs, including 10 American citizens and one lawful permanent resident, brought suit in the U.S. District Court for the District of Massachusetts, after CBP or ICE searched their electronic devices when they reentered the country following business or personal travel.

The plaintiffs included a military veteran, journalists, students, a NASA space engineer and a business owner.

The plaintiffs alleged violations of their Fourth Amendment rights, arguing that the warrantless searches of their electronic devices violated their constitutional right to protection against unreasonable searches and seizures. They additionally challenged the CBP and ICE policies as "facially violative of the Fourth Amendment's protection against unreasonable searches and seizures."[12]

In November 2019, the federal court ruled in Alasaad that border agents may conduct a search — whether basic or advanced — of a traveler's electronic device only if they have reasonable suspicion based on a "showing of specific and articulable facts, considered with reasonable inferences drawn from those facts," that the device contains digital contraband.[13]

The decision requires a higher threshold of suspicion to conduct a basic search of electronic devices than do CBP and ICE policies and matches the existing agency standard for an advanced search.

In reaching its decision, the court found that, in the case of searches of electronic devices — which could contain:

> photographs, contact information, emails and text messages ... prescriptions, employment information, travel history and internet browsing history ... [e]ven under the border search exception ... the privacy interests implicated by unfettered access to such a trove of personal information ... must be balanced against the promotion of paramount governmental interests at the border.[14]

In weighing that balance, the Alasaad court relied heavily on Riley v. California, the landmark 2014 case in which the Supreme Court held:

> The police generally may not, without a warrant, search digital information on a cell phone seized from an individual who has been arrested.[15]

In Riley, which considered the rights of an arrestee, the Supreme Court found that even "diminished privacy interests do ... not mean that the Fourth Amendment falls out of the picture entirely."[16]

Applying the Riley analysis, the Alasaad court found that the record supporting the government's interest in conducting searches under the border search exception was sparser.[17] The court also rejected the government's comparison between the searches at issue and the "broad latitude border officials have to search physical items," concluding that digital evidence or contraband is not like physical items or even travelers themselves.[18]

The court concluded that:

> Unlike a vehicle, vessel or even a home at the border, ... the data stored on a cell phone is distinguished from physical records by quantity alone, [but] certain types of data are also qualitatively different. ... It can reveal an individual's private interests or concerns as evidenced by internet search and browsing history, reveal where a person has been through historic location information, and reveal which files a person created, accessed and when he or she did so through metadata. The potential level of intrusion from a search of a person's electronic devices simply has no easy comparison to non-digital searches.[19]

On that basis, the court concluded that reasonable suspicion — but not probable cause — is required to conduct a border search of an electronic device.

The U.S. Court of Appeals for the Ninth Circuit, U.S. Court of Appeals for the Fourth Circuit and U.S. Court of Appeals for the Eleventh Circuit have similarly addressed this issue post-Riley, but have disagreed as to the level of suspicion needed for border searches of electronic devices.

In U.S. v. Cano, the Ninth Circuit held that the border search exception "authorizes warrantless searches of a cell phone only to determine whether the phone contains contraband."[20] The defendant in that case was stopped by CBP while driving across the border from Mexico into the U.S.[21]

During the stop, CBP located more than 30 pounds of cocaine in the defendant's car and subsequently seized and manually reviewed his cellphone before conducting a logical download and review of data on the defendant's phone using specialized software.[22] The court concluded that manual search of the defendant's phone was permissible at first, but that the subsequent forensic search of the phone exceeded what is allowed without reasonable suspicion.[23]

The Ninth Circuit distinguished between a manual search — a "quick look unintrusive search" that is "reasonable without even particularized suspicion" — and a forensic search — "essentially a computer strip search."[24]

In contrast to Alasaad, which required reasonable suspicion for all border searches of electronic devices, the Cano court concluded that manual searches require no suspicion, while "the forensic examination of a cell phone requires a showing of reasonable suspicion."[25]

Likewise, in U.S. v. Kolsuz, the Fourth Circuit held that some measure of individualized suspicion is required for a nonroutine border search — like a forensic border search of a phone — but did not reach the question of whether that standard should be reasonable suspicion or probable cause.[26]

In Kolsuz, customs agents detained the defendant as he was about to board a flight to

Turkey at Washington Dulles International Airport because they had found firearms parts in his luggage.[27] The customs agents arrested the defendant before they took "possession of his smartphone and subjected it to a month-long, off-site forensic analysis, yielding a nearly 900-page report cataloguing the phone's data."[28]

The Fourth Circuit concluded the search was appropriate, finding that a showing of reasonable suspicion had been made and that the agent who conducted the search "reasonably relied on precedent holding that no warrant was required."[29] The court concluded:

> The justification behind the border search exception is broad enough to accommodate not only the direct interception of contraband as it crosses the border, but also the prevention and disruption of ongoing efforts to export contraband illegally, through searches initiated at the border.[30]

In contrast to Alasaad, Cano and Kolsuz — each of which found that reasonable suspicion was required for at least some border searches of electronic devices — in U.S. v. Touset, the Eleventh Circuit saw "no reason why the Fourth Amendment would require suspicion for a forensic search of an electronic device when it imposes no such requirement for a search of other personal property."[31]

In Touset, the court concluded that CBP agents appropriately searched electronic devices belonging to the defendant after he arrived at the Atlanta airport on an international flight.[32] The search took place because prior investigative efforts had suggested that the defendant was involved with child pornography.[33]

CBP manually inspected and returned the defendant's two iPhones and his camera, but detained his two laptops, two external hard drives, and two tablets, and employed computer forensic analysts to search those devices.[34] The search revealed child pornography on the laptops and external hard drives.[35]

The court concluded that the searches would have been permissible even in the absence of reasonable suspicion:

> Although it may intrude on the privacy of the owner, a forensic search of an electronic device is a search of property. And our precedents do not require suspicion for intrusive searches of any property at the border.[36]

Against the backdrop of what may be an emerging, post-Riley circuit split, both the government and the plaintiffs have appealed the district court's decision in Alasaad to the U.S. Court of Appeals for the First Circuit.

The government argues that CBP and ICE directives allowing for warrantless searches do not violate the Fourth Amendment and the district court erred in requiring reasonable suspicion for all searches of electronic devices.[37]

For their part, the plaintiffs have appealed as well, arguing that reasonable suspicion is insufficient, and that federal agents should be required to obtain a warrant supported by probable cause to search a person's electronic device at the border.[38] The First Circuit is set to hear oral arguments in the case at the start of the new year.

The U.S. Court of Appeals for the Fifth Circuit may also add its voice to this emerging split,

as oral arguments were held this month in Anibowei v. Morgan, a case in which the appellant has similarly argued that a probable cause warrant should be required for searches of cellphones at the border.[39]

In that case, the appellant — an attorney and a U.S. citizen — sued several federal law enforcement agencies based on allegations that his phone has been the subject of five border searches at airports.[40]

The government has argued that neither the Fifth Circuit nor the Supreme Court required a warrant for a border search of a cellphone, and that such searches are permissible under the border search exception.[41]

While the government's brief notes that Ninth and Fourth Circuits have required reasonable suspicion for certain border searches of cellphones, the government did not take a position on the issue of reasonable suspicion, contending that it has not been meaningfully raised or briefed, either at the trial court or on appeal.[42]

Practical Considerations

While the outcome of the appeals in Alasaad and Anibowei at this point remain unknown, it is likely that the Supreme Court may need to settle the emerging circuit split about the constitutional standard for searching an electronic device at the border.

In the meantime, however, the increase in CBP and ICE searches of electronic devices at the border raises practical questions for educational institutions, companies, and other organizations whose academics, researchers, students, and employees travel to or from the U.S.

These organizations should consider implementing guidance regarding such travel. What follows are practical considerations that may assist in developing that guidance.

During a border search, federal agents have broad latitude to ask questions about a range of topics, including travel itineraries and visa status. A U.S. citizen or permanent legal resident is only required to answer questions establishing their identity and status, while visa holders and other travelers may be barred from entering the U.S. if they refuse to answer an agent's questions.

Nevertheless, travelers should know that they have the right to not answer an agent's questions, and that if they choose to answer, anything they say could be used against them.

Even if a border search of a phone must be supported by reasonable suspicion, that suspicion may be developed at any time prior to the beginning of the search. An agent does not need to have reasonable suspicion prior to the traveler's arrival at the airport. Reasonable suspicion may be developed during a stop or interview based on various factors, including statements the traveler makes in response to an agent's questions.

Electronic devices subject to search include not only laptops and cellphones, but also other electronic storage devices, including flash drives, portable hard drives and SIM cards.

Travelers should consider traveling with clean electronic devices that do not contain all of their personal electronic data. Clean phones or laptops contain just the electronic data that is needed for the upcoming trip. Therefore, if phones or laptops are seized, they can be quickly reviewed and returned, and there is no risk of losing sensitive personal information.

If traveling with an employer-owned device, travelers should consider carrying a letter from their employer confirming the traveler is authorized to possess all the information on the device.

Travelers are not required to provide passwords to allow agents to access their electronic devices. Failure to do so, however, may result in agents seizing a device and holding it for a longer period of time, as they attempt to access it through other means.

Under CBP policy, the detention of a device ordinarily should not exceed five days. In practice, however, it may take months before a device is returned. The policy has many exceptions that allow for longer detainments, including the need to unlock a password-protected device.

Border stops and searches may last long enough for travelers to miss their flights. Agents are not required to end a stop or search in time for a traveler to make their flight, and the U.S. government will not reimburse travelers for related expenses.

CBP policy requires agents to issue a traveler a receipt after seizing their device.

The seizure of an electronic device does not necessarily mean that the owner of the device is under criminal investigation, though agents may later develop evidence supporting a criminal prosecution based on information on the device.

George Varghese is a partner, and Benjamin Conery and Sierra Shear are senior associates, at WilmerHale.

[1] https://www.wilmerhale.com/en/insights/publications/20200324-the-china-initiative-heads-to-school.

[2] See U.S. v. Ramsey, 431 U.S. 606, 620 (1977).

[3] See Alasaad v. Nielsen, 419 F. Supp. 3d 142, 156 (D. Mass. 2019).

[4] See id.

[5] Id. at 155.

[6] Ramsey, 431 U.S. at 618.

[7] See Alasaad, 419 F. Supp. 3d at 148–49.

[8] Id.

[9] Id.

[10] See Terry v. Ohio, 392 U.S. 1 (1968).

[11] See https://www.cbp.gov/newsroom/national-media-release/cbp-releases-statistics-electronic-device-searches-0.

[12] See Alasaad, 419 F. Supp. 3d at 154.

[13] Id. at 166.

[14] Id. at 161.

[15] Riley v. California, 573 U.S. 373, 392 (2014).

[16] Id. at 401.

[17] Alasaad, 419 F. Supp. at 162.

[18] Id.

[19] Id. at 163 (internal quotation marks and citations omitted).

[20] U.S. v. Cano, 934 F.3d 1002, 1018 (9th Cir. 2019).

[21] Id. at 1008.

[22] Id. at 1008-09.

[23] Id. at 1019-20.

[24] Id. at 1015 (internal quotation marks omitted).

[25] Id. at 1015-16.

[26] U.S. v. Kolsuz, 890 F.3d 133, 137 (4th Cir. 2018), as amended (May 18, 2018).

[27] Id. at 136.

[28] Id.

[29] Id.

[30] Id.

[31] U.S. v. Touset, 890 F.3d 1227, 1233 (11th Cir. 2018).

[32] Id. at 1230.

[33] Id.

[34] Id.

[35] Id.

[36] Id. at 1234.

[37] See Corrected Appellants' Principal Brief, Alasaad v. Wolf, Case No. 20-1077 (1st Cir. June 1, 2020).

[38] See Plaintiffs' Principal and Response Brief, Alasaad v. Wolf, Case No. 20-1077 (1st Cir. July 31, 2020).

[39] See Brief of Appellant, Anibowei v. Morgan, et al., Case No. 20-10059 (5th Cir. June 1, 2020).

[40] See id.

[41] See Brief of Appellees Anibowei v. Morgan, et al., Case No. 20-10059 (5th Cir. July 22, 2020).

[42] See id.