NISKANEN CENTER

IMMIGRATION POLICY BRIEF
Rights at the Border

by Kristie De Peña

July 2017

Introduction

All travelers entering the United States, including U.S. citizens, participate in routine customs processing that includes examinations of baggage, electronics, and cars. The impacts of those searches depend—in part—on who is entering, where they're coming from, and their current immigration status.

Generally, U.S. citizens have the most protections and cannot be denied admission; however, their electronic devices can be detained for months. Foreign visitors have the fewest rights; if denied admission, many have no constitutional right to procedural due process—like notice and a hearing—to challenge their exclusion. Legal permanent residents—green card holders—have more constitutional protections than a visitor, but fewer than a U.S. citizen. If they're denied admission, they likely have a constitutional right to procedural due process under the Fifth Amendment, but may ultimately be denied admission.

As protecting the border becomes an increasingly important aspect of national security, and the federal government seeks more and more information as a condition of admission, a plethora of issues arise revolving around individual rights at the border, like searches of electronic devices and guidelines for storing information collected from those devices.

Current Policy

The legal foundation for border searches, regardless of their type, capacity, or format, is well-established.[1]

[1] Title 19 of the United States Code, § § 482, 1467, 1496, 1581 and 1582 provides that all persons, baggage, and other merchandise arriving in or leaving the United States are subject to inspection and search by Customs and Border Patrol (CBP) officers. Various laws enforced by CBP, including 8 United States Code (U.S.C.) 1357, 19 U.S.C. § § 482, 1581, 1582, authorize such searches. The Supreme Court has also upheld this authority. *See United States v. Flores-Montano*, 541 U.S. 149 (2004); *United States v. Montoya de Hernandez*, 473 U.S. 531 (1985).

Generally, the Fourth Amendment requires that a search or seizure conducted by a governmental agent be reasonable and supported by probable cause. The Supreme Court has interpreted the Fourth Amendment to include a presumptive warrant requirement on all searches and seizures conducted by the government. Any violation of these requirements can result in the suppression of any information derived therefrom. However, in the interests of sovereignty and national security, a border search exception was carved out of the Fourth Amendment.

Border Search Exception

Few exceptions to the presumptive warrant and probable cause requirements are more firmly rooted than the "border search"exception.[2] Derived from the sovereign right to stop and examine persons and property crossing into the country, border searches allow customs officials the flexibility to inspect incoming individuals and their belongings.

Throughout history, a number of Supreme Court decisions have found that U.S. Customs and Border Patrol's (CBP) search authority is unique, and the Court has long recognized situations that render obtaining a warrant impractical or against the public's interest. Accordingly, various exceptions to the warrant and probable cause requirements of the Fourth Amendment now exist.

Courts have determined that border searches usually fall into two categories—routine and non-routine. Generally, the distinction between a routine and non-routine search turns on the level of intrusiveness. Routine border searches are reasonable simply by virtue of the fact that they occur at the border and consist of only a limited intrusion, while non-routine searches generally require "reasonable suspicion" and vary in technique and intrusiveness. For a non-routine search, a border agent needs individualized suspicion about the traveler, or a factual reason to believe a specific person is involved in criminal activity.

In all cases, searches must not be discriminatory or motivated by a traveler's appearance.

Border Search Intersection with Technology

Most individuals have a significant privacy interest in all the data that modern digital devices contain, including call logs, emails, text messages, voicemails, browsing history, calendar entries, contact lists, shopping lists, personal notes, photos and videos, geolocation logs, and

[2] 19 U.S.C. § 482 for customs officials and Immigration and Nationality Act (INA) § 287 (codified in 8 U.S.C. § 1357) for immigration officers and addresses the scope of the government's constitutional authority to search and seize persons and property at the border. Several bills before the 111th Congress addressed border searches: two of which, H.R. 239 (the Securing our Borders and our Data Act of 2009) and H.R. 1726 (the Border Security Search Accountability Act of 2009), address border searches of laptops and other electronic storage devices. H.R. 1900 would provide emergency deployments of federal officers to the border and would authorize funds to local law enforcement to stem the illegal trafficking of firearms into Mexico. S. 205, H.R. 495, and H.R. 1448 would also authorize funds for Bureau of Alcohol, Tobacco, Firearms, and Explosives agents to interdict the illegal trafficking of firearms to Mexico.

other personal files. In nearly every case, an individual crossing the border will carry some type of digital or electronic device.

In 2016, almost 24,000 electronic devices were searched at border, a huge jump from the nearly 5,000 devices that were searched in 2015. The pace of searches continues to accelerate, with the Department of Homeland Security reportedly conducting 5,000 device searches in February 2017 alone. Given that digital devices like smartphones and laptops contain highly personal information and provide access to more highly personal information stored in the cloud, many are looking at the legality of border searches to determine how whether searches of electronic devices are routine or non-routine. Some guidance is available in recent court decisions.

In 2013, the Ninth Circuit held that border agents need reasonable suspicion of illegal activity before they could conduct a forensic search, aided by sophisticated software, of the defendant's laptop. The court also held that a manual search of a digital device is routine and therefore is acceptable under the Fourth Amendment, without a warrant or suspicion.

In *Riley v. California* (2014), the Supreme Court held that the police must have probable cause and obtain a warrant to search the cellphone of an individual under arrest. The police argued that the warrantless and suspicionless cell phone search was permissible as a "search incident to arrest." However, the Court held that "a warrant is generally required before such a search, even when a cell phone is seized incident to arrest." However, it is critical to note that *this reasoning hasn't been applied in the border context*. At this point, it is unlikely that that this ruling will apply at the border.

Further, given the ubiquity of cloud computing, the government's reach into private data becomes even more concerning. In the cloud, a user's data, including the same kind of highly sensitive data one would have in papers at home, is held on remote servers rather than on the device itself. The digital device is a conduit to retrieving information from the cloud, akin to the key to a safe deposit box. Notably, although the virtual "safe deposit box" does not itself cross the border, it may appear as a seamless part of the digital device when presented at the border.

Self-Incrimination: Fingerprints and Passwords

The Fifth Amendment is also an important consideration in the border search context, because it may confer protections against being required to divulge passwords or provide fingerprints to access the contents of electronic devices.

The Fifth Amendment guarantees that "no person shall be... compelled... to be a witness against himself." Statements and actions that qualify as bearing "witness" are called "testimonial." A person's statement or action is testimonial if it would disclose the contents of their mind,

meaning that generally, an individual does not need to provide testimony revealing the contents of his mind that could be incriminatory.

Only a judge—not a border agent—can decide whether the Fifth Amendment protects unlocking a device, providing a password, or disclosing social media information information. However, a border agent can certainly determine whether to seize a device, or to deny admission.

At least one court has held that the Fifth Amendment confers an absolute right to refuse to provide one's password to unlock or decrypt a digital device. Other courts have adopted a weaker test, under which the government need only show that the individual knows the password. Border agents usually find it easier to show that a traveler knew the password of the device they carried, as compared to showing that the individual knew a particularly suspect file was in that device.

Many experts believe that a fingerprint lock is just as protective as a password, but it is, in fact, less secure—both legally and technically—than passwords. Some courts (though not all) have held that fingerprints, unlike passwords, are not part of the contents of our minds, and thus fall outside Fifth Amendment protection.

However, law enforcement and border agents are working to bypass those considerations. Police are developing technologies that can take a person's stored fingerprint from a government database and use it to unlock that person's phone, and border agents may force a traveler to place their finger to their phone to open it.

In both the Fourth and Fifth Amendment contexts, the law is changing slowly, but Congress can expedite these necessary protections by legislating them in advance of court decisions.

Considerations for Future Policy

We need a framework of changes that are bipartisan enough to move through Congress, and are the outcome of pragmatic, thoughtful discussions that consider all the available information—statistics, history, morality, experience, and law. Below are a number of considerations to inform future policy:

- Law enforcement officials often try to persuade persuade people to consent to searches, which makes it harder to challenge those searches in court. Sometimes law enforcement officials achieve so-called "consent" by being vague about whether they are asking or ordering a civilian to do something. Consent allows agents to look at all of the content stored in a device, manually or with powerful forensic software, look at cloud content it it's accessible through your device, and to copy and store all of this content for later use.

Laws protecting both law enforcement and individuals are necessary to ensure compliance that satisfies national security concerns, but also protect sensitive information. For example, attorneys must be allowed to protect files to protect attorney-client privilege, but immigration officials must also have access to relevant information that potentially has national security implications.

- Similarly, even with refusal to comply with an order to unlock a device, provide a password, or disclose social media information, border agents may seize devices or copy the encrypted contents of devices.There must be a protocol whereby individuals can obtain information about the return of their seized devices and relevant information about what information the government may have stored or copied.
- Flagging individuals for heightened screening is also an issue that is increasingly becoming concerning. There must be protections in place allowing an individual to refute their classification in cases where there is a mistake or where such classification is unwarranted.
- The intersection of the First, Fifth, and Fourteenth Amendment at the border must be regularly reviewed and assessed to ensure that additional searches are not based on the traveler's religion, ethnicity, or similar characteristics.

Conclusion

Protecting individual rights at the border is as important as protecting our sovereign border. We must vigilantly continue to improve the processes and mechanisms at the border so as not to infringe on individual rights or reduce the efficiency and efficacy of our precautionary policies. Policy guiding individual rights and searches at the border must be carefully considered to avoid government overreach, inadvertent loss of data, and to ensure that all individuals entering the U.S. are thoroughly screened.