Class 7: Privacy at the Border

Background law on searches at the border

1. There has long been an exception to the Fourth Amendment for searches that take place at the border

    a. The Supreme Court has held that, generally speaking, "routine" searches that take place at the border are reasonable by virtue of the fact that they take place at the border.

    b. These kinds of searches do not require:

        i. Any kind of suspicion

        ii. Or any kind of prior judicial approval

    c. This applies at the border and also the "functional equivalent" (e.g., international airports, fixed checkpoints near the border)

2. This is true at least for "routine" searches, but what's "routine"?

    a. *United States v. Flores-Montano*, 541 U.S. 149 (2004)

        i. **Facts:** Customs officials seized 37 kilograms of marijuana from Manuel Flores-Montano's gas tank at the international border.

            1. Driving a 1987 Ford Taurus station wagon through a port of entry in southern California.

            2. Initial inspection conducted. Then car taken to secondary inspection. Customs inspector tapped on the gas tank, noted that it sounded "solid," and asked for a mechanic to inspect it.

                a. "Within 20 to 30 minutes, the mechanic arrived. He raised the car on a hydraulic lift, loosened the straps and unscrewed the bolts holding the gas tank to the undercarriage of the vehicle, and then disconnected some hoses and electrical connections. After the gas tank was removed, the inspector hammered off bondo (a putty-like hardening substance that is used to seal openings) from the top of the gas tank. The inspector opened an access plate underneath the bondo and found 37 kilograms of marijuana bricks. The process took 15 to 25 minutes."

        ii. **Held:** "We hold that the search in question did not require reasonable suspicion."

1. “But the reasons that might support a requirement of some level of suspicion in the case of highly intrusive searches of the person—dignity and privacy interests of the person being searched—simply do not carry over to vehicles.”

2. “The Government’s interest in preventing the entry of unwanted persons and effects is at its zenith at the international border.”

3. Time and again, we have stated that “searches made at the border, pursuant to the longstanding right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border.” *United States v. Ramsey*, 431 U. S. 606, 616 (1977).

3. Non-“routine” searches can require some individualized suspicion

    a. *United States v. Montoya de Hernandez*, 473 U.S. 531 (1985)

        i. **Facts:** Detention of an individual suspected of carrying drugs in her gastrointestinal tract. Detained for nearly 24 hours, and officers eventually obtained a warrant to conduct an examination, which turned up balloons containing heroin.

        ii. **Held**:

            1. We hold that the detention of a traveler at the border, beyond the scope of a routine customs search and inspection, is justified at its inception if customs agents, considering all the facts surrounding the traveler and her trip, reasonably suspect that the traveler is smuggling contraband in her alimentary canal.

            2. “particularized and objective basis”

    b. Lower courts have applied the same logic to other intrusive searches, including

        i. Strip searches; body cavity searches; x-ray searches

    c. *United States v. Ramsey*, 431 U.S. 606 (1977)

        i. **Facts:** Warrantless search of international letter based on “reasonable cause to suspect” it contained undeclared merchandise or contraband

            1. Investigation of an international heroin-smuggling operation.

            2. Two individuals based in Thailand were arrested for their part, and then: “Two days after this arrest . . . a United States customs officer in New York City, without any knowledge of the foregoing events, inspecting a sack of incoming international mail from

Thailand, spotted eight envelopes that were bulky and which he believed might contain merchandise."

3. A customs officer opened the envelopes and conducted a field test of the white powder he found inside.

ii. **The challenge**: The defendant challenged admission of the evidence, arguing that the government should've obtained a warrant based on probable cause.

iii. **Held**:

1. Border searches generally reasonable because they take place at the border

a. "That searches made at the border, pursuant to the long-standing right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border, should, by now, require no extended demonstration."

b. Border searches, then, from before the adoption of the Fourth Amendment, have been considered to be "reasonable" by the single fact that the person or item in question had entered into our country from outside. There has never been any additional requirement that the reasonableness of a border search depended on the existence of probable cause. This longstanding recognition that searches at our borders without probable cause and without a warrant are nonetheless "reasonable" has a history as old as the Fourth Amendment itself.

2. History supports this view

a. **The first customs statute, enacted in 1789 (several months before proposing the Bill of Rights):** granted customs officials "full power and authority" to enter and search "any ship or vessel, in which they shall have reason to suspect any goods, wares or merchandise subject to duty shall be concealed . . .."

3. Does not matter that the item being searched was a letter:

a. It is clear that there is nothing in the rationale behind the border-search exception which suggests that the mode of entry will be critical.

b. It was conceded at oral argument that customs officials could search, without probable cause and without a warrant, envelopes carried by an entering traveler, whether in his luggage or on his person. Tr. of Oral Arg. 43-44. Surely no different constitutional standard should apply simply because the envelopes were mailed not carried.

4. First Amendment does not protect the letter:

    a. Nor do we agree that, under the circumstances presented by this case, First Amendment considerations dictate a full panoply of Fourth Amendment rights prior to the border search of mailed letters.

    b. [**key caveat**] Here envelopes are opened at the border only when the customs officers have reason to believe they contain other than correspondence, while the reading of any correspondence inside the envelopes is forbidden.

Searches of electronic devices at the border

1. What about searches of electronic devices at the border?

    a. Are these routine searches that can be undertaken without suspicion?

    b. Or are they non-routine because of how invasive they may be?

2. CBP Policy

    a. Basic searches: Anything that isn't an advanced search.

    b. Advanced searches:

        i. **What:** An advanced search is 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.

        ii. **When:** reasonable suspicion of activity in violation of the laws enforced or administered by CBP, or in which there is a national security concern, and with supervisory approval at the Grade 14 level or higher (or a manager with comparable responsibilities)

    c. **Remotely stored data.** May not intentionally access data stored remotely. Will request that traveler disable network connection.

    d. **Privileged information**. Segregate data claimed to be privileged; search using a Filter Team. Delete after review unless materials indicate "an imminent threat to

homeland security" (or needed for a litigation hold "or other requirement of law").

e. **Other sensitive data**. "Other possibly sensitive information, such as medical records and work-related information carried by journalists, shall be handled in accordance with any applicable federal law and CBP policy."

f. **Encrypted data**.

    i. "Travelers are obligated to present electronic devices and the information contained therein in a condition that allows inspection of the device and its contents."

    ii. If unable to access b/c of encryption or passcode, can detain the device.

    iii. [Note: a little unclear what the practical effect of this "obligat[ion]" is, but may depend on citizenship.]

g. **Detention.** Can detain "for a brief, reasonable period of time to perform a thorough border search." Typically "should not exceed five (5) days."

h. **Destruction of data.** If no P/C to seize the device or information contained therein, must destroy the data

    i. "probable cause to believe that the device, or copy of the contents from the device, contains evidence of a violation of law that CBP is authorized to enforce or administer."

3. Are these policies constitutional? Start with *Riley*.

4. *Riley v. California* (2014)

    a. **Question**: whether the police may, without a warrant, search digital information on a cell phone seized from an individual who has been arrested.

    b. **Facts**: searches of cellphones incident to lawful arrest

    c. **Background**:

        i. For a long time, the Court has recognized an exception to the Fourth Amendment's warrant requirement for searches *incident to a lawful arrest*

            1. Exception set out mainly in two cases:

            2. *Chimel* (1969) — police may search area within immediate control of an arrestee to ensure their safety and prevent the destruction of evidence

3. *Robinson* (1973) — held that the search-incident-to-arrest exception was categorical and did not depend upon a case-by-case assessment of the likelihood that weapons or evidence would be found on the arrestee.

4. [*Gant* (2009) — extending the exception to vehicles, with an additional extension (related to the discovery of evidence) unique to the searches of vehicles.]

d. **Discussion**:

i. How to apply *Chimel* and *Robinson* to device searches?

1. Court rejects a "mechanical application"

a. "a mechanical application of Robinson might well support the warrantless searches at issue here."

2. Looks instead to the underlying rationales of *Robinson*

a. But while Robinson's categorical rule strikes the appropriate balance in the context of physical objects, neither of its rationales has much force with respect to digital content on cell phones.

3. Held that the underlying rationales do not apply

4. Key foundations of the ruling:

a. Risk to police officers:

i. "Digital data stored on a cell phone cannot itself be used as a weapon to harm an arresting officer or to effectuate the arrestee's escape."

b. Preservation of evidence:

i. "And once law enforcement officers have secured a cell phone, there is no longer any risk that the arrestee himself will be able to delete incriminating data from the phone."

ii. What about "remote wiping and data encryption":

1. "With respect to remote wiping, the Government's primary concern turns on the actions of third parties who are not present at the scene of arrest. And data encryption is

even further afield. There, the Government focuses on the ordinary operation of a phone's security features, apart from any active attempt by a defendant or his associates to conceal or destroy evidence upon arrest."

2. "We have also been given little reason to believe that either problem is prevalent."

3. **[Faraday bag]** In any event, as to remote wiping, law enforcement is not without specific means to address the threat. Remote wiping can be fully prevented by disconnecting a phone from the network. There are at least two simple ways to do this: First, law enforcement officers can turn the phone off or remove its battery. Second, if they are concerned about encryption or other potential problems, they can leave a phone powered on and place it in an enclosure that isolates the phone from radio waves.

c. Privacy interests:

i. The United States asserts that a search of all data stored on a cell phone is "materially indistinguishable" from searches of these sorts of physical items. Brief for United States in No. 13-212, p. 26. That is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together. Modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse.

e. **Key takeaway**: Supreme Court refused to extend the search-incident-to-arrest exception from the warrant requirement to searches of cellphones ***because the balance of interests comes out differently***

5. **Key question going forward**: does similar logic suggest that the border-search exception should not apply to searches of electronic devices at the border

a. Courts have analyzed this question by breaking it into multiple parts:

i. Whether a manual search requires any level of suspicion or prior approval?

ii. Whether an advanced/forensic search requires any level of suspicion or prior approval?

iii. What may border agents search for (i.e., what is the purpose of the exception)? Just enforcement of customs laws (e.g., contraband), or also general law enforcement?

6. What have courts said about **basic/manual searches**

    a. Every court to have addressed the question (1st, 4th, 9th, 11th Circuits) has held that manual inspections are "routine" and so may be conducted without any suspicion

7. What have courts said about **advanced searches**

    a. One court has held that no suspicion is required (11th Circuit)

    b. Most courts have held that reasonable suspicion required b/c not "routine" (4th and 9th Circuits)

    c. One judge in dissent has said she would require a warrant (11th Circuit dissent in *Vergara*)

8. What have courts said about the **permissible purposes** of border searches

    a. 9th Circuit in *Cano* — "cell phone searches at the border, whether manual or forensic, must be limited in scope to a search for digital contraband"

    b. 1st Circuit in *Alasaad* —

        i. Plaintiffs had argued "that the border search exception (a) extends only to searches aimed at *preventing the importation of contraband or entry of inadmissible persons* and (b) *covers only searches for contraband itself*, rather than for evidence of border-related crimes or contraband."

        ii. **Held**: the border search exception is not limited to searches for contraband itself rather than evidence of contraband or a border-related crime.

9. **Other questions not directly answered by the courts**:

    a. Can the government force those crossing the border to unlock their devices or decrypt their data?

    b. Can the government retain copies of the data? For how long and for what purposes?

10. [**just for reference**] Cases:

    a. *United States v. Vergara*, 884 F.3d 1309 (11th Cir. 2018) (Forensic searches do not require a warrant or probable cause. Border searches have never been subject to the warrant and probable cause requirements, and so the only question is whether they might require reasonable suspicion; but don't need to address that question in this case b/c defendant didn't challenge district court's finding of reasonable suspicion. Dissent by Judge Jill Pryor; would have held that forensic search requires a warrant.)

    b. *United States v. Touset*, 890 F.3d 1227 (11th Cir. 2018) ("no suspicion is necessary to search electronic devices at the border")

    c. *United States v. Cano*, 934 F.3d 1002 (9th Cir. 2019) ("we conclude that manual cell phone searches may be conducted by border officials without reasonable suspicion but that forensic cell phone searches require reasonable suspicion. We clarify *Cotterman* by holding that 'reasonable suspicion' in this context means that officials must reasonably suspect that the cell phone contains digital contraband. We further conclude that cell phone searches at the border, whether manual or forensic, must be limited in scope to a search for digital contraband.")

Are the border-search cases relevant to other searches of digital data at the border?

1. What's the most significant other stream of data across our borders?

    a. International communications, including the Internet!

2. Does the border-search doctrine apply to these communications?

    a. A little bit unclear.

        i. Electronic surveillance is generally governed by two very complicated statutory regimes — the Wiretap Act and FISA

        ii. Depending on how precisely the government carried out the surveillance, and what precise information it wanted to collect from which particular communications — the surveillance might be governed by those regimes.

            1. If so, then the border-search doctrine isn't so much relevant to the government's *substantive authority*, although it might be relevant to the *constitutionality* of that authority.

            2. For example, if the government wanted to acquire the contents of a U.S. person's international communications, and it carried out the acquisition on U.S. soil, that would qualify as "electronic surveillance" within the meaning of FISA.

3. And so the "border search" exception wouldn't necessarily do much work in defining the scope of the government's authority, because FISA already does

iii. But, might be relevant to constitutionality of that authority:

1. *See* Government's brief in the *Muhtorov* case ("Although the government does not contend that the Section 702 collection here was per se reasonable under the border search doctrine, the point remains that the principles underlying that doctrine support the constitutional reasonableness of the collection at issue in this case because, at a minimum, privacy expectations are sharply reduced in their context.")

b. Also, for surveillance that doesn't qualify as "electronic surveillance" within the meaning of FISA, the border-search doctrine could very well be extremely important

i. E.g., Transit Authority

3. You can see how the exact parameters of the border-search-doctrine's application to digital data is extremely important:

a. Whether any kind of suspicion is required

b. Whether prior judicial approval is required

c. What interests the doctrine serves

4. What about encryption of data?

a. Presumably, it will make — and perhaps has already made — much of this kind of searching less useful, at least when it comes to the content of communications

b. Could the border-search doctrine provide a basis for insisting on backdoors for cross-border communications?

Free speech at the border

1. <u>Domestically</u>:

a. Social media registration requirement

i. The policy

1. Outgrowth of "extreme vetting"

2. Under the Trump administration, DOS instituted a rule requiring nearly all individuals who apply for U.S. visas from abroad to

register their social media handles with the government (May 31, 2019)

a. Applies to a list of 20 social media platforms, and to all handles used on those platforms for the last 5 years

3. Retention and dissemination of the data

a. Stored in A-files (which can last for 100 years after date of birth)

4. Government argues that the requirement helps it confirm the identity and admissibility of visa applicants

ii. Our legal challenge:

1. KFAI filed a legal challenge to the requirement on behalf of Doc Society and the International Documentary Association

2. We argue that it causes several injuries:

a. It chills expression by visa applicants and potential visa applicants by causing them to hesitate before posting anything critical of the U.S. using a handle that they will be required to disclose to customs authorities

b. It creates a more acute risk for those who use pseudonymous handles, because they are not otherwise associated with their accounts.

3. Legal claims

a. APA / First Amendment

4. Government's responses:

a. No Article III standing — among other arguments: no chill b/c social media profiles are generally public and often associated with your real identities

b. Failure to state a claim

i. APA — committed to agency discretion and so not judicially reviewable

ii. First Amendment — plenary authority over policies and rules for exclusion of aliens

1. Whether under *Mandel* (facially legitimate and bona fide) or under a lower form of scrutiny

2. Right to be forgotten

    a. The EU court ruling most people associate with the "right to be forgotten" was an interpretation of the predecessor to the GDPR, the Data Protection Directive (1995).

        i. **Article 12**: Member States shall guarantee every data subject the right to obtain from the controller: … (b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive"

    b. *Google v. Spain* (ECJ 2014)

        i. **Facts**: Spanish individual filed a complaint with Spain's DPA against Google, asking it to de-index an article concerning the individual.

        ii. **Key questions analyzed**:

            1. Is a search engine a data "processor" w/in the meaning of the Directive?

                a. Yes, even though the processing is automatic; even though the processing is done w/o regard to personal nature of the data; and even though the data at issue was already published by 3rd party (i.e., the newspaper)

            2. Is a search engine a "controller" of the data contained in the web pages it indexes?

                a. Yes, for more or less the same reasons

            3. May the DPA order Google to de-index an item?

                a. **Google said**: go to the underlying website, not to us!

                b. **Court:** search engines are particularly important to privacy: "processing of personal data … carried out by the operator of a search engine is liable to affect significantly the fundamental rights to privacy … when the search by means of that engine is carried out on the basis of an individual's name, since that processing enables any internet user to obtain through the list of results a structured overview of the information relating to that individual that can be found on the internet"

i. Especially true b/c search engines are gateways, and hard to track down all the original publishers

c. **Held:** "the supervisory authority or judicial authority may order the operator of the search engine to remove from the list of results displayed following a search made on the basis of a person's name links to web pages published by third parties containing information relating to that person"

4. In what circumstances is an individual entitled to de-indexing of information he considers prejudicial?

a. Where the information is "inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing at issue carried out by the operator of the search engine"

c. Now there is a more developed "right to be forgotten" in the GDPR (May 25, 2018)

i. **Article 17**: "Right to erasure ('right to be forgotten')"

1. "right to obtain from the controller the erasure of personal data concerning him or her without undue delay," where one of these circumstances is present:

a. Data no longer necessary for purposes for which they were collected or processed

b. Data subject withdraws consent (and no other legal ground for processing)

c. Etc.

2. Key exception: "shall not apply to the extent that processing is necessary: (a) for exercising the right of freedom of expression and information"

d. The latest ruling — *Google v. France* (2019)

i. In 2015, French Data Protection Authority ruled that when Google grants a de-listing request under the RTBF, it must de-index the website from all domain name extensions (i.e., not just www.google.fr)

1. Google refused to comply; just de-listed from the relevant domain

2. French DPA rejected geo-blocking alternative that Google proposed

ii. CJEU reversed.

iii. First, it observed that it is important for the EU to have the authority to require de-listing on all versions of a search engine, given that globalized internet access can cause the harms that the GDPR is concerned with.

iv. But, second, the RTBF is not absolute:

    1. Moreover, the right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality (see, to that effect, judgment of 9 November 2010, Volker und Markus Schecke and Eifert, C-92/09 and C-93/09, EU:C:2010:662, paragraph 48, and Opinion 1/15 (EU- Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, point 136). Furthermore, the balance between the right to privacy and the protection of personal data, on the one hand, and the freedom of information of internet users, on the other, is likely to vary significantly around the world.

v. And given the balance and different approaches taken outside the EU, the court held that Google cannot be forced to de-list around the world based on granting a standard de-listing request.

    1. But, can be forced to de-list decision w/r/t all Member States

    2. And member states can force de-listing around the world, because nothing in EU law prohibits it.