Courthouse News Service

Committee Examines Border Patrol's Phone Searches

Brandi Buchman

July 11, 2018

Warrantless cellphone searches by Customs and Border Patrol agents at the northern and southern borders of the United States have exploded a long-brewing constitutional crisis, a panel of legal experts told a Senate Homeland Security subcommittee Wednesday.

Since 2009, policy at Customs and Border Patrol, or CPB, has not required agents to obtain a warrant or have "reasonable suspicion" before asking a traveler to unlock their phone or electronic device if they are stopped at the border.

According to Georgetown University law professor Laura Donahue's testimony Wednesday in Washington, D.C., CPB's policy has done more than prompt the predictable series of lawsuits alleging civil rights violations and racial profiling.

CPB's policy has led to skyrocketing searches and a total breakdown in constitutional rights available to migrants and U.S. citizens alike travelling over the U.S.'s borders, Donahue said.

In 2015, CPB reported it had examined 8,500 devices. That figure doubled in 2016 before "soaring to more than 30,000 searches in 2017," Donahue told members of the senate subcommittee on Federal Spending Oversight and Emergency Management.

At Immigration and Customs Enforcement, agents reported searching over 4,400 phones in 2015. In 2016, they searched nearly six times that amount with 23,000 devices reportedly searched.

In January, CPB made minor changes to its policy, stipulating that agents distinguish searches as "basic" or "advanced" to avoid possible Fourth Amendment violations.

A "basic" search allows an agent to manually review a device's contents – anything that can be scrolled through on a phone is fair game. But a search becomes "advanced" when an agent has reasonable suspicion and needs to equip the person's phone or laptop with another device to conduct a more thorough forensic analysis.

Even with this change to policy, if a CPB agent believes "national security" is at stake, the reasonable suspicion requirement vanishes.

The executive branch has failed to resolve this loophole, Senator Rand Paul said Wednesday.

Paul also noted the search directives at ICE haven't been updated since 2012. As it stands, ICE or CPB can keep devices for 30 days, then extend the confiscation for 15 days at a time – indefinitely.

The searches may have an unintended effect, Matthew Feeney, director of the Cato Institute's project on emerging technologies, told lawmakers.

Ostensibly denying all visitors and travelers their rights at U.S. borders creates a hostile atmosphere, he explained.

"Knowing that your phone has gone to a backroom and has been searched by officers will change people's behavior," Feeney said.

The Cato Institute is a think tank devoted to preserving individual liberties and limited government.

Both Feeney and Donahue noted that the agencies offer no assurances about how they store or retain data once they've searched a device.

"Leaving it to CPB and ICE to police themselves is quite dangerous," Donahue said. She went on to reference an observation from the Supreme Court case *Riley v. California,* a unanimous decision finding that warrantless search and seizure of digital content on a cellphone during an arrest is unconstitutional.

"'The founders did not fight a revolution to gain the right to government agency protocols,'" Donahue quoted from the Supreme Court's opinion. "It was a profound point. This is about rights, they should be statutorily guaranteed and not left up to whomever heads that organization or agency in terms of their regulation."

The policies are being used as an "end-run" around the warrant process, said Neema Singh Guliani, senior legislative counsel with the American Civil Liberties Union.

Agents who want to go after targets further inland need only wait for them to get within 100 miles of the border to justify using CPB's policy.

"The weakness is in the guidance [of the policy]," Guliani said. "The guidance doesn't prohibit searches from being used for general law enforcement purposes as an end-run around the constitution. It doesn't prohibit searches performed at the request of or to assist other law enforcement agencies. Then there are questions about oversight and compliance for limited protections… how do we know they're actually being followed by an agency? There's not a lot of confidence that is even happening."

Cellphone searches at the border present a unique problem since the quantity and type of information found on a device is dramatically different from what a person can have searched in a single suitcase when crossing a border.

"There's medical information, political affiliation, religious beliefs… all types of information that is extraordinarily sensitive. [A phone] is the equivalent of someone arriving at the border with more than just a suitcase but an entire house of information," Guliani said.

Legislators have introduced two bills in the senate they believe will resolve the loopholes. The Leahy-Daines bill places restrictions on searches and seizures of electronic devices at the border. A more comprehensive bill tackling data sensitivity, known as the Protecting Data at the Border Act, would hand down more specific regulations. The latter legislation would prohibit the government from accessing any cellphone data without a warrant and would bar denial of entry or exit based on a person's refusal to disclose access to a device.