


Ruling May Stop Willy-Nilly Gadget Searches at US Borders

Por Yael Grauer

Wired.com, 12 mayo 2015.



Laptop computers, left at TSA checkpoints at Newark Liberty International Airport, sit in a locked cabinet at the TSA office January 6, 2015 in Union, NJ.  KATHERINE FREY/THE WASHINGTON POST/GETTY IMAGES

THERE'S LONG BEEN a sense that the 4th amendment's protection from unreasonable search and seizure doesn't apply at the border. And in certain ways, it doesn't. Reasonable expectations of privacy are held to different standards. Routine searches that would otherwise be considered unreasonable are permitted due to the "border search exception" to the 14th amendment's due process requirement. And people entering the country, as well as their property, can be searched without a warrant, probable cause, or even reasonable suspicion. In addition, courts have previously upheld willy-nilly searches of laptops and phones along the US border.

But a new ruling by Amy Berman Jackson, a federal judge on the United States District Court for D.C., is signaling a different direction for search guidelines at the border, at least as far as laptops and mobile devices are concerned.

Given the vast storage capacity of even the most basic laptops, and the capacity of computers to retain metadata and even deleted material, one cannot treat an

electronic storage device like a handbag simply because you can put things in it and then carry it onto a plane. — Amy Berman Jackson

Here's what happened: Korean businessman Jae Shik Kim's laptop was seized at the border, and evidence was harvested by the Department of Homeland Security, which made a forensic image, or duplicate copy, and searched the entire contents of his laptop aided by specialized forensic software. The purpose was to gather additional evidence for a preexisting investigation.

But the court granted a motion to suppress the evidence. It determined that the search was unreasonable because of a lack of reasonable suspicion of ongoing or imminent criminal activity, and because the search was so invasive of Kim's privacy.

"The Supreme Court has said in a number of opinions that 4th Amendment protections are reduced at the border, but it has been clear to also say that the 4th Amendment does not disappear at the border. The border is not a constitution-free zone," Nathan Freed Wessler, a Staff Attorney with ACLU's Speech, Privacy, and Technology Project, told WIRED.

The case is the third of its kind. In 2013, a 9th Circuit court concluded that laptops and other electronic storage devices may not be subject to forensic examination without a reason for suspicion. In 2014, a District Court in Maryland determined that reasonable suspicion was needed to justify a forensic search of electronic data storage devices.

"I think what's important is that it adds to the growing consensus that digital information triggers different legal requirements, or that it requires a different sort of analysis, in that you can't just analogize to a backpack. Your suitcase and your clothes are not the same thing as your computer," said Hanni Fakhoury, Senior Staff Attorney at the Electronic Frontier Foundation.

For years, hackers, activists, journalists and even filmmakers have been searched upon reentry to the United States and had their laptops and devices confiscated. David House and Jacob Appelbaum were both detained and had their devices seized for mere association with WikiLeaks. (House won a lawsuit against DHS.) Academy-award winning American documentary filmmaker and journalist Laura Poitras was repeatedly detained going over the US border, and had her mobile phone, laptop, and notes confiscated. These types of searches typically require that laptops and/or devices be sent to a facility with teams of forensic analysts, and it can take weeks for the analysis to be complete. In addition to the privacy violation, having laptops and smartphones seized for that long can be enormously disruptive.

To be clear, warrants are not required for any types of searches along the border. And cursory searches—when US Customs and Border Protection agents open a laptop in front of you or the room next to you, or click into your smartphone and do

a quick visual search or perfunctory search of a term or two—are still permitted without any suspicion whatsoever.

“Where the protection is starting to come is when the government seizes the device, and then downloads from it the complete or near complete content of the laptop or the smartphone, and then can subject it to forensic search techniques, or invasive searches of every email and every photo and every word document and every calendar entry, even of deleted files and of operating files that aren’t even visible to the user. It’s those kinds of searches that these courts are saying are so categorically more invasive than anything law enforcement has ever been able to do before that they require higher protections,” said Wessler. Making controversial statements, being affiliated with groups the government dislikes, or lawfully receiving information from whistleblowers (without conspiring in aiding them to break a law) do not in themselves constitute reasonable suspicion of a crime. This court decision raises the bar from the kind of at-their-whim searches the government has sometimes conducted.

Although the ruling does not set a binding precedent for lower courts, Fakhoury explained that it is a persuasive precedent. “It adds to the growing body of cases saying that there are problematic privacy concerns when it comes to computer searches and that it triggers differing kinds of 4th amendment analysis,” he said. Courts looking for persuasive evidence may look to these cases for guidance.