

## US border agents are doing 'digital strip searches'. Here's how to protect yourself

By [Olivia Solon](#)

The Guardian.com, 14 Jul 2017

The number of mobile phones being searched at the US border is exploding, but certain steps can help secure your privacy



Searches of mobile phones by US border agents grew from fewer than 5,000 in 2015 to 25,000 in 2016. Photograph: JGI/Tom Grill/Getty Images/Blend Images

Last month, the US-born Nasa engineer [Sidd Bikkannavar was pulled into additional screening when he entered the US](#) after a two-week vacation in Chile. He was taken into a room and told to hand over his phone and passcode. He explained that the phone belonged to Nasa and contained important work-related data, but immigration officials insisted and handed him a document explaining that the penalty for refusing was “detention”. He eventually complied and they took his phone into a another room for 30 minutes before allowing him to leave.

Bikkannavar never found out why he was chosen for additional screening. He had not travelled to any of the [Muslim-majority countries included in Trump's travel ban](#).

Cases like this are exploding. According to data from the Department of Homeland Security (DHS), searches of mobile phones by border agents grew from fewer than 5,000 in 2015 to 25,000 in 2016 (DHS told the Guardian that there was an anomaly in the 2016 data, but did not reveal how that changes these figures). Anecdotal

evidence indicates that searches have risen further in the wake of the election of Donald Trump.

Border agents carry out these invasive searches without any warrant or even suspicion, going through text messages, social media accounts and photos, while asking the owner about the people they are interacting with, their religious affiliations and travel patterns.

Experts credit the rise in searches to the increase in technical capacity at the border.

“They are building capacity to routinely search as many devices as possible,” said Alex Abdo, senior staff attorney at the Knight First Amendment Institute at Columbia University.

The lack of transparency over the process has led the free speech watchdog [to file a freedom of information lawsuit](#), seeking to obtain the DHS’s rules for “suspicionless” searches of mobile devices. The institute wants to know what exactly immigration officials are looking for and how they decide who to target.

“There’s a basic privacy concern with forcing people to be subjected to a digital strip-search simply for having crossed the nation’s borders,” said Abdo.

Christina Sinha, staff attorney at the Asian Law Caucus, added: “It’s a ridiculous situation. The entire thing is terrible. All it’s doing is greatly exacerbating the racial profiling problem at the border.” She provides legal representation for those unjustly affected by sweeping national security policies, many of whom are Muslims.

“People are incredibly vulnerable at the border,” she said. “People are coming off 20-hour flights, completely jet-lagged and stuck in this limbo land of the border and there’s an armed agent in front of you preventing you from coming into the country.”

In addition to going through people’s smartphones in person, US Customs and Border Protection (CBP) and US Immigration and Customs Enforcement (Ice) can also [confiscate devices for a further forensic examination](#). In this case agents can make full copies of all of the data on the phone, which can be shared with other government agencies. DHS has published test results from [dozens of tools](#) it can use to extract data from phones.



A customs officer screens an arriving passenger in Houston, Texas. Photograph: Dave Einsel/Getty Images

This gives rise to business concerns, particularly if devices used for work contain confidential information that could be copied and potentially leaked.

“If someone works for a company in Silicon Valley and has trade secrets on their work laptop, we recommend they speak with their supervisor at work before they travel,” said Sinha.

What if individuals refuse to give over their passwords? Depending on your immigration status, that could mean being turned away from the United States.

But “US citizens and returning green card holders can’t be denied entry for refusing to provide a password,” said Esha Bhandari, a staff attorney at the American Civil Liberties Union (ACLU).

If your device is seized and if your goal is to prevent border officials from accessing your data, experts recommend using encryption and a strong password.

However, it’s important to keep in mind that failure to cooperate can create practical problems. Immigration officials can detain people for hours of secondary questioning and seize their device for weeks. “They can make your life very inconvenient every time you travel,” said Abdo.

For those entering the country on a visa or visa waiver, refusal to comply with border officials can mean being turned away or even having your immigration status revoked.

**So what can people do to protect their personal data?**

“The ideal thing to do is to leave your main phone and laptop at home and go across the border with a burner phone,” said Sinha, referring to a simple device that doesn’t have your email or social media apps on it.

For those who can’t do that, experts suggest deleting data and apps from devices.

“With so much of our data now stored in the cloud rather than on the local device, apps have become the prime conduit to our data,” explained Paul Lipman, the Silicon Valley-based CEO of the security company Bullguard.

He offers the example of the secure cloud storage app Dropbox, where he keeps personal and business documents. To prevent these types of documents from being searched by border agents, a smartphone owner can simply delete the app and download it again once they are in the country. “A hassle? Yes. But hardly a big one.”

A CBP spokeswoman said the searches affected less than one hundredth of 1% of travelers to the US and that they were “often integral to a determination of an individual’s intentions upon entry”.

“They are critical to the detection of evidence relating to terrorism and other national security matters, human and bulk cash smuggling, contraband, and child pornography. They can also reveal information about financial and commercial crimes, such as those relating to copyright, trademark and export control violations,” she said.

### **Since you’re here ...**

... we have a small favour to ask. More people are reading the Guardian than ever but advertising revenues across the media are falling fast. And unlike many news organisations, we haven’t put up a paywall – we want to keep our journalism as open as we can. So you can see why we need to ask for your help. The Guardian’s independent, investigative journalism takes a lot of time, money and hard work to produce. But we do it because we believe our perspective matters – because it might well be your perspective, too.

*I appreciate there not being a paywall: it is more democratic for the media to be available for all and not a commodity to be purchased by a few. I’m happy to make a contribution so others with less means still have access to information. Thomasine, Sweden*

If everyone who reads our reporting, who likes it, helps fund it, our future would be much more secure. **For as little as €1, you can support the Guardian – and it only takes a minute. Thank you.**