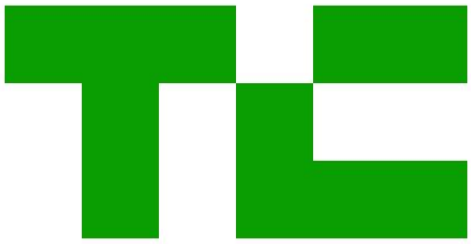

The new electronic police state

Matthew Feeney

September 24, 2017

According to the government, your privacy protections evaporate the moment you set foot in an airport.

Although the Fourth Amendment protects us and our "effects" from "unreasonable searches and seizures," Customs and Border Protection agents can take advantage of an exception to this constitutional protection and search our electronic devices at airports without first establishing reasonable suspicion or securing a warrant.

It's a problem that's only getting worse. Last week the American Civil Liberties Union and the Electronic Frontier Foundation entered into a suit on behalf of eleven travelers against the Department of Homeland Security. The plaintiffs claim that warrantless and suspicionless border electronic device searches violate the First and Fourth Amendments.

They're absolutely right. CBP agents are gaining access to massive troves of personal information related to law-abiding Americans. This exception is an affront to everyone's privacy and must be revoked.

For example, earlier this year Sidd Bikkannavar, an engineer at NASA's Jet Propulsion Laboratory, was subject to a secondary airport inspection at the airport in Houston, and was asked by a customs and border patrol agent for the passcode to a phone he was carrying.

The phone belonged to NASA, and although Bikkannayar explained as much, the agent continued asking for the code. Fearing that CBP would seize the phone and that he would miss his connecting flight to Los Angeles, Bikkannavar relented and provided it.

After around 30 minutes the agent returned with the phone, telling Bikkannavar the phone had been analyzed with "algorithms" and that no "derogatory" information had been found.

The idea that the border or airport is a region of reduced privacy expectations is not new. As Justice Rehnquist noted in the 1977 case *United States v. Ramsey*, the same Congress that proposed the Bill of Rights passed the United States' first customs statute, giving officials the authority to search "any ship or vessel, in which they shall have reason to suspect any goods, wares or merchandise subject to duty shall be concealed."

It was also in *Ramsey* that Rehnquist declared, "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 should, by now, require no extended demonstration."

Yet today, unlike 1977 or 1789, more than three quarters of American adults own smartphones. These devices contain vast amounts of data related to our personal and professional lives. CBP policy does not allow agents to access information housed on remote servers, but even a search of information resident on an electronic device can uncover videos, texts, photos and reveal what apps someone has downloaded.

These apps can expose dating habits as well as religious affiliations. Thanks to current policy, any traveler could be coerced into allowing CBP to access this private information without any suspicion that they have violated immigration law.

CBP searches of electronic devices are relatively rare, but the number of such searches has been increasing over the last few years. These searches do not always target travelers from terrorist hotspots, either. Bikkannayar is an American citizen and member of the Border Protection Global Entry program, which is designed for what CBP describes as "pre-approved, low-risk travelers."

Earlier this year then-DHS Secretary John Kelly discussed, among other things, these electronic device searches at a Senate Homeland Security and Governmental Affairs Committee hearing. While some might think that the warrantless searches of electronic devices may be a valuable counter-terrorism tactic, Kelly did not cite a single instance where an electronic device search had lead to a terrorism charge or conviction.

As the recent ACLU and Electronic Frontier Foundation suit shows, these searches have disrupted the lives and violated the privacy of a NASA engineer, a former Air Force Captain, a Harvard graduate student, a nursing student, and entrepreneurs, all citizens with no connections to terrorist activity.

It's important that the federal government keep us safe from foreign threats, and CBP should be able to examine phones and laptops belonging to people who are the subject of a warrant. But CBP should not have the authority to go on fishing expeditions for incriminating data, harassing and intimidating citizens and permanent residents without any evidence of wrongdoing.