The Border Is a Back Door for U.S. Device Searches

By SUSAN STELLIN

Newly released documents reveal how the government uses border crossings to seize and examine travelers' electronic devices instead of obtaining a search warrant to gain access to the data.

The documents detail what until now has been a largely secretive process that enables the government to create a travel alert for a person, who may not be a suspect in an investigation, then detain that individual at a border crossing and confiscate or copy any electronic devices that person is carrying.

To critics, the documents show how the government can avert Americans' constitutional protections against unreasonable search and seizure, but the confiscations have largely been allowed by courts as a tool to battle illegal activities like drug smuggling, child pornography and terrorism.

The documents were turned over to David House, a fund-raiser for the legal defense of Chelsea Manning, formerly known as Pfc. Bradley Manning, as part of a legal settlement with the Department of Homeland Security. Mr. House had sued the agency after his laptop, camera, thumb drive and cellphone were seized when he returned from a trip to Mexico in November 2010. The data from the devices was then examined over seven months.

Although government investigators had questioned Mr. House about his association with Private Manning in the months before his trip to Mexico, he said no one asked to search his computer or mentioned seeking a warrant to do so. After seizing his devices, immigration authorities sent a copy of Mr. House's data to the Army Criminal Investigation Command, which conducted the detailed search of his files. No evidence of any crime was found, the documents say.

"Americans crossing the border are being searched and their digital media is being seized in the hopes that the government will find something to have them convicted," Mr. House said. "I think it's important for business travelers and people who consider themselves politically inclined to know what dangers they now face in a country where they have no real guarantee of privacy at the border."

A spokeswoman from Customs and Border Protection said the agency declined to comment about the settlement with Mr. House, or answer questions about travelers' rights when their devices are seized or inspected during a border crossing.

While many travelers have no idea why they are singled out for a more intrusive screening at a border, one of the documents released in Mr. House's settlement shows that he was flagged for a device search months before he traveled to Mexico.

On July 8, 2010, Immigration and Customs Enforcement investigators in New York created an alert, known as a TECS lookout, for Mr. House, noting that he was "wanted for questioning re leak of classified material" and ordering border agents to "secure digital media" if he appeared at an inspection point.

TECS is a computer system used to screen travelers at the border, and includes records from law enforcement, immigration and antiterrorism databases. A report from the Department of Homeland Security about border searches of electronic devices says a traveler may be searched "because he is the subject of, or person-of-interest-in, an ongoing law enforcement investigation and was flagged by a law enforcement 'lookout' " in the Immigration and Customs Enforcement computer system.

On Oct. 26, 2010, an automated message notified investigators that Mr. House had an airline reservation on Oct. 30, traveling on American Airlines flight 865 from Dallas-Fort Worth to Los Cabos, Mexico; a later query noted that he would be returning to Chicago O'Hare on American flight 228, landing at 6 p.m. on Nov. 3.

Since airline passengers are required to provide carriers with their birth date and passport number before a flight to or from the United States, and airlines pass that information to Homeland Security (as part of the Advance Passenger Information System), computers matched the lookout alert with Mr. House's itinerary. Agents were then dispatched to meet him.

"It is clear from these documents that the search of David House's computers had nothing to do with protecting the border or with enforcing immigration laws," said Catherine Crump, a lawyer with the American Civil Liberties Union, which represented Mr. House along with the A.C.L.U. of Massachusetts. "The government used its broader powers at the border to conduct a search of House's devices that no court would have approved."

The documents, released by the A.C.L.U. on Monday, also detail the extent of the government's examination of Mr. House's computer. After a search using 183 keywords that turned up more

than 26,000 files, the investigation concluded that “no data was found that constituted evidence of a crime.”

As part of the settlement, the government agreed to destroy all copies of the data taken from Mr. House, and update his file so he will not automatically be detained when he returns to the United States after traveling abroad, which has happened repeatedly since 2010.

Courts have largely supported the government’s authority to search electronic devices when travelers, including citizens, enter the United States. The so-called border search exception to the Fourth Amendment is based on the government’s interest in thwarting illegal activities.

But in March, the Court of Appeals for the Ninth Circuit in California set a new limit on device searches at the border, ruling in United States v. Cotterman that reasonable suspicion of criminal activity was required for a forensic search of a device — for instance, using software to analyze encrypted or deleted data, as opposed to performing a more cursory look at documents, photos or other files.

Customs and Border Protection, part of the Department of Homeland Security, said that it conducted electronic media searches on 4,957 people from Oct. 1, 2012, through Aug. 31, 2013, or about 15 a day, which is similar to the average during the previous two years. About 930,000 people are screened daily by border agents.

But for those pulled aside for a secondary inspection (about 35,000 travelers a day), the experience can be distressing, resulting in a missed connecting flight, a prolonged interrogation, and in Mr. House’s case, the loss of a laptop necessary for his livelihood.

“I was worried about losing my job, and not being able to pay my rent, and what I was going to tell my parents,” said Mr. House, 26, who was working as a computer programmer at the time. He was also concerned about the government getting access to names stored on his laptop of individuals who had donated money to Private Manning’s legal defense. Private Manning was sentenced by a military judge last month to 35 years in prison for providing more than 700,000 government files to WikiLeaks.

Mr. House’s lawsuit was among a handful of cases challenging the government’s authority to search devices at the border. Pascal Abidor, a graduate student in Islamic studies, sued the government after he was detained and his laptop was seized during an Amtrak trip from Montreal to New York in 2010. A decision in that case is expected soon, according to the case manager for Judge Edward R. Korman, who is writing the opinion for the United States District

Court for the Eastern District of New York. Mr. Abidor is also being represented by Ms. Crump of the A.C.L.U.

For now, the law remains murky about any limits on intrusive border inspections, including how long travelers can be detained, whether they are required to provide passwords for their devices — Mr. House refused — and whether they must answer any question an agent asks. Responses may be recorded in a traveler's TECS file and shared with other government agencies.