CSEC used airport Wi-Fi to track Canadian travellers: Edward Snowden documents

30. Januar 2014

By Greg Weston, Glenn Greenwald, Ryan Gallagher, CBC News

A top secret document retrieved by U.S. whistleblower Edward Snowden and obtained by CBC News shows that Canada's electronic spy agency used information from the free internet service at a major Canadian airport to track the wireless devices of thousands of ordinary airline passengers for days after they left the terminal.

After reviewing the document, one of Canada's foremost authorities on cyber-security says the clandestine operation by the Communications Security Establishment Canada (CSEC) was almost certainly illegal.

Ronald Deibert told CBC News: "I can't see any circumstance in which this would not be unlawful, under current Canadian law, under our Charter, under CSEC's mandates."

The spy agency is supposed to be collecting primarily foreign intelligence by intercepting overseas phone and internet traffic, and is prohibited by law from targeting Canadians or anyone in Canada without a judicial warrant.

As CSEC chief John Forster recently stated: "I can tell you that we do not target Canadians at home or abroad in our foreign intelligence activities, nor do we target anyone in Canada. "In fact, it's prohibited by law. Protecting the privacy of Canadians is our most important principle."

But security experts who have been apprised of the document point out the airline passengers in a Canadian airport were clearly in Canada.

CSEC said in a written statement to CBC News that it is "mandated to collect foreign signals intelligence to protect Canada and Canadians. And in order to fulfill that key foreign intelligence role for the country, CSEC is legally authorized to collect and analyze metadata."

Metadata reveals a trove of information including, for example, the location and telephone numbers of all calls a person makes and receives - but not the content of the call, which would legally be considered a private communication and cannot be intercepted without a warrant.

"No Canadian communications were (or are) targeted, collected or used," the agency says.

In the case of the airport tracking operation, the metadata apparently identified travelers' wireless devices, but not the content of calls made or emails sent from them.

Black Code

Deibert is author of the book Black Code: Inside the Battle for Cyberspace, which is about

internet surveillance, and he heads the world-renowned Citizen Lab cyber research program at the University of Toronto's Munk School of Global Affairs.

He says that whatever CSEC calls it, the tracking of those passengers was nothing less than an "indiscriminate collection and analysis of Canadians' communications data," and he could not imagine any circumstances that would have convinced a judge to authorize it.

A passenger checks his cellphone while boarding a flight in Boston in October. The U.S. Federal Aviation Administration issued new guidelines under which passengers will be able to use electronic devices from the time they board to the time they leave the plane, which will also help electronic spies to keep tabs on them.

The latest Snowden document indicates the spy service was provided with information captured from unsuspecting travellers' wireless devices by the airport's free Wi-Fi system over a two-week period.

Experts say that probably included many Canadians whose smartphone and laptop signals were intercepted without their knowledge as they passed through the terminal.

The document shows the federal intelligence agency was then able to track the travellers for a week or more as they - and their wireless devices - showed up in other Wi-Fi "hot spots" in cities across Canada and even at U.S. airports.

That included people visiting other airports, hotels, coffee shops and restaurants, libraries, ground transportation hubs, and any number of places among the literally thousands with public wireless internet access.

The document shows CSEC had so much data it could even track the travellers back in time through the days leading up to their arrival at the airport, these experts say.

While the documents make no mention of specific individuals, Deibert and other cyber experts say it would be simple for the spy agency to have put names to all the Canadians swept up in the operation.

All Canadians with a smartphone, tablet or laptop are "essentially carrying around digital dog tags as we go about our daily lives," Deibert says.

Anyone able to access the data that those devices leave behind on wireless hotspots, he says, can obtain "extraordinarily precise information about our movements and social relationships."

Trial run for NSA

The document indicates the passenger tracking operation was a trial run of a powerful new software program CSEC was developing with help from its U.S. counterpart, the National Security Agency.

In the document, CSEC called the new technologies "game-changing," and said they could be used for tracking "any target that makes occasional forays into other cities/regions."

Sources tell CBC News the technologies tested on Canadians in 2012 have since become fully operational.

CSEC claims "no Canadian or foreign travellers' movements were 'tracked,'" although it does not explain why it put the word "tracked" in quotation marks.

Deibert says metadata is "way more powerful than the content of communications. You can tell a lot more about people, their habits, their relationships, their friendships, even their political preferences, based on that type of metadata."

The document does not say exactly how the Canadian spy service managed to get its hands on two weeks' of travellers' wireless data from the airport Wi-Fi system, although there are indications it was provided voluntarily by a "special source."

The country's two largest airports - Toronto and Vancouver - both say they have never supplied CSEC or other Canadian intelligence agency with information on passengers' Wi-Fi use.

Alana Lawrence, a spokesperson for the Vancouver Airport Authority, says it operates the free Wi-Fi there, but does "not in any way store any personal data associated with it," and has never received a request from any Canadian intelligence agency for it.

A U.S.-based company, Boingo, is the largest independent supplier of Wi-Fi services at other Canadian airports, including Pearson International in Toronto.

Spokesperson Katie O'Neill tells CBC News: "To the best of our knowledge, [Boingo] has not provided any information about any of our users to the Canadian government, law enforcement or intelligence agencies."

It is also unclear from the document how CSEC managed to penetrate so many wireless systems to see who was using them - specifically, to know every time someone targeted at the airport showed up on one of those other Wi-Fi networks elsewhere.

Deibert and other experts say the federal intelligence agency must have gained direct access to at least some of the country's main telephone and internet pipelines, allowing the mass-surveillance of Canadian emails and phone calls.

'Blown away'

Ontario's privacy commissioner Ann Cavoukian says she is "blown away" by the revelations.

"It is really unbelievable that CSEC would engage in that kind of surveillance of Canadians. Of us.

"I mean that could have been me at the airport walking around… This resembles the activities of a totalitarian state, not a free and open society."

Experts say the document makes clear CSEC intended to share both the technologies and future information generated by it with Canada's official spying partners - the U.S., Britain, New Zealand and Australia, the so-called Five Eyes intelligence network.

Indeed, the spy agency boasts in its leaked document that, in an apparently separate pilot project, it obtained access to two communications systems with more than 300,000 users, and was then able to "sweep" an entire mid-sized Canadian city to pinpoint a specific imaginary target in a fictional kidnapping.

The document dated May 2012 is a 27-page power-point presentation by CSEC describing its airport tracking operation.

While the document was in the trove of secret NSA files retrieved by Snowden, it bears CSEC's logo and clearly originated with the Canadian spy service.

Wesley Wark, a renowned authority on international security and intelligence, agrees with Deibert.

"I cannot see any way in which it fits CSEC's legal mandate."

Wark says the document suggests CSEC was "trying to push the technological boundaries" in part to impress its other international counterparts in the Five-Eyes intelligence network.

"This document is kind of suffused with the language of technological gee-whiz."

Wark says if CSEC's use of "very powerful and intrusive technological tools" puts it outside its mandate and even the law, "then you are in a situation for democracy where you simply don't want to be."

Like Wark and other experts interviewed for this story, Deibert says there's no question Canada needs CSEC to be gathering foreign intelligence, "but they must do it within a framework of proper checks and balances so their formidable powers can never be abused. And that's the missing ingredient right now in Canada."

The only official oversight of CSEC's spying operations is a retired judge appointed by the prime minister, and reporting to the minister of defence who is also responsible for the intelligence agency.

"Here we clearly have an agency of the state collecting in an indiscriminate and bulk fashion all of Canadian communications and the oversight mechanism is flimsy at best," Deibert says.

"Those to me are circumstances ripe for potential abuse."

CSEC spends over $400 million a year, and employs about 2,000 people, almost half of whom are involved in intercepting phone conversations, and hacking into computer systems supposedly in other countries.

It has long been Canada's most secretive spy agency, responding to almost all questions about its operations with reassurances it is doing nothing wrong.

Privacy watchdog Cavoukian says there has to be "greater openness and transparency because without that there can be no accountability.

"This trust-me model that the government is advancing and CSEC is advancing – 'Oh just trust us, we're doing the right thing, don't worry' - yes, worry! We have very good reason to worry."

In the U.S., Snowden exposed massive metadata collection by the National Security Agency, which is said to have scooped up private phone and internet records of more than 100 million Americans.

A U.S. judge recently called the NSA's metadata collection an Orwellian surveillance program

that is likely unconstitutional.

The public furor over NSA snooping prompted a White House review of the American spy agency's operations, and President Barack Obama recently vowed to clamp down on the collection and use of metadata.

Cavoukian says Canadians deserve nothing less.

"Look at the U.S. - they've been talking about these matters involving national security for months now very publicly because the public deserves answers.

"And that's what I would tell our government, our minister of national defence and our prime minister: We demand some answers to this."