Returning travellers made to hand over phones and passcodes to Australian Border Force

Sydney man says he doesn't know what officials looked at on his phone or what happens to his data

Josh Taylor
Tue 18 Jan 2022 03.30 AEDT

A man who was forced to hand over his phone and passcode to Australian Border Force after returning to Sydney from holiday has labelled the tactic "an absolute gross violation of privacy", as tech advocates call for transparency and stronger privacy protections for people's devices as they enter the country.

Software developer James and his partner returned from a 10-day holiday in Fiji earlier this month and were stopped by border force officials at Sydney airport. They were taken aside, and after emptying their suitcases, an official asked them to write their phone passcodes on a piece of paper, before taking their phones into another room.

It was half an hour before their phones were returned, and they were allowed to leave. James initially posted about his ordeal on Reddit.

"We weren't informed why they wanted to look at the phones. We were told nothing," he told Guardian Australia.

"Who knows what they're taking out of it? With your phone and your passcode they have everything, access to your entire email history, saved passwords, banking, Medicare, myGov. There's just so much scope."

James said he has no idea what officials looked at, whether a copy of any of the data was made, where it would be stored and who would have access to it.

"It's an absolute gross violation of privacy."

Under the Customs Act, ABF officers can force people to hand over their passcodes to allow a phone search, as part of their powers to examine people's belongings at the border, including documents and photos on mobile phones.

A spokesperson for ABF did not respond to specific questions about James' case, nor questions on how often the power is used or where the data is stored.

The spokesperson said people can be questioned and their phone searched "if they suspect the person may be of interest for immigration, customs, biosecurity, health, law-enforcement or national security reasons".

"The ABF exercises these powers in order to protect the Australian community from harm and deliver upon its mission to protect Australia's border and enable legitimate travel and trade. Information seized from passengers phones has contributed to the success of many domestic law enforcement operations targeting illegal activities," the spokesperson said.

"If an individual refuses to comply with a request for an examination of their electronic device, they may be referred for further law enforcement action."

Within Australia's borders, there are more hurdles for law enforcement to access devices, including needing a warrant before people can be compelled to unlock their phones.

In 2016, Nine newspapers reported a man sued ABF after text messages were sent and then deleted from his phone by an official while they had possession of his phone at the border in 2014.

A freedom of information request in 2016 revealed the department had apologised to the man in 2015, and had determined the counter-terrorism unit officer breached ABF's code of conduct.

Electronic Frontiers Australia chair Justin Warren said it is impossible to determine how common such searches of phones are because the department doesn't release any data on it – unlike data on warrants obtained under other domestic surveillance laws.

"There is no transparency, and the authorities prefer it that way. Anecdotally, it seems to happen quite a lot," Warren said, adding it showed the need for stronger privacy rights in Australia.

"This is just another example of how few rights Australians actually have. We need a Bill of Rights in Australia to prevent abuses like this, and real consequences for abuse when it happens."

Samantha Floreani, program lead at Digital Rights Watch, agreed.

“This is a prime example of the kind of privacy violations that can occur when you don’t have fundamental human rights,” she said. “A federal charter of human rights is long overdue in Australia.

“It is completely unreasonable that people should be subject to such an invasion of privacy without so much as an explanation.”

Warren advised people flying into Australia not to have anything on their device that they don’t want authorities accessing, and to ensure their device is encrypted with a strong passcode.

“Once they take your device out of your sight, you should assume it’s completely compromised and they have a copy of everything that was on it, and act accordingly,” he said.

Warren stressed that people in such a situation should also seek legal advice.

James said the incident made him rethink what he would do next time he travels out of Australia.

“I think what I’ll just do next time is as we fly into Sydney, I’ll just press the factory reset button on the phone and when they pull me up again, I’ll be handing them a fresh clean factory reset.”