SENATE STANDING COMMITTEE ON LEGAL AND CONSTITUTIONAL AFFAIRS
ADDITIONAL BUDGET ESTIMATES
14 FEBRUARY 2022

Home Affairs Portfolio
Australian Border Force

Program 3.2: Border Management

AE22-050 - ABF Officer powers in relation to electronic devices

Senator Nick McKim asked:

Senator McKIM: Commissioner Outram, I had some questions for you on the same matter that Senator Patrick was asking you about before dinner, which was the confiscation of phones and electronic devices at borders. I understand you took a number of those questions on notice, which is fine. If you need to take these questions on notice too I completely understand. Do your officers have the power to manipulate data on somebody's phone that they take? Can they add data or delete data or change data or copy data from people's phones or computers?
Mr Outram: No, is my understanding. I will take it on notice and confirm for you what exact powers they have in relation to electronic devices for arriving passengers.
Senator McKIM: Thank you, I'd appreciate that. As part of that, could you also take on notice, please, whether, if there are any powers—I presume there are powers to copy data, for example. You used the example before dinner of child pornography. I presume, if you found some, you would have the power to copy that.
Mr Outram: Indeed. You either seize the phone or you download data.
Senator McKIM: Does the relevant data, if you did download data, have to be relevant to the belief the officer had, in terms of his or her reason for seizing the phone in the first place? I'm happy if you answer that on—
Mr Outram: I'll take it on notice but I'll give you context. It's a bit similar to questions by Senator Sheldon. In this day and age, when you're searching electronic devices, there could be terabytes of data, and the only way to sift through it is electronically. So you may well download data that isn't of interest, in terms of your reasonable grounds to suspect for a particular thing, and you don't have the time to pour over terabytes of data to find the thing you're after. You have to run searches.
Senator McKIM: So you might download a wide range of data for the purpose of searching—
Mr Outram: Indeed, and there are strict rules about how you handle and manage that data.
Senator McKIM: Anything more you can provide, on notice, would be appreciated. If you wish to take this on notice, that's fine. Do you have the powers to compel someone to provide their passcode or password to a device?
Mr Outram: I think the secretary answered that earlier but I'll take it on notice. We'll provide you a definitive view of our powers at the border in relation to these devices.
Senator McKIM: Thank you. The story that Senator Patrick was referring to, which has now been tabled, quotes a spokesperson for the ABF as saying: '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.' Specifically, I'm asking whether a request for the examination of an electronic device would capture not just the handing over of

the device but the provision of a password or passcode.
Mr Outram: I'll take it all on notice, thank you.

Answer:

Policy Framework

The Australian Border Force (ABF) has powers under the *Customs Act 1901* (Customs Act), the *Migration Act 1958* (Migration Act) and the *Maritime Powers Act 2013* (Maritime Powers Act) to examine and copy electronic devices which includes mobile phones, computers and removable storage devices such as USB drives.

Under Section 186 of the Customs Act, Australian Border Force (ABF) officers have the power to examine all goods at the border, including electronic documents on mobile phones and other personal electronic devices.

Section 252 of the Migration Act allows any property, including electronic devices, under the immediate control of a person, in certain circumstances, to be searched for evidence for grounds for cancelling the person's visa. This authority also allows copies of documents to be made for this purpose.

The ABF does not have the power to access cloud or online services without a judicial warrant at the border.

The ABF will only seize a mobile phone under the Customs Act that it suspects on reasonable grounds to be special forfeited goods. Special forfeited goods include prohibited imports and exports such as objectionable material on devices in digital formats. Objectionable material includes, among other items, illegal pornography, terrorism related material and media that has been, or would be, refused classification. It is an offence under Australian law to import or export prohibited goods and the penalty can be up to 10 years imprisonment.

Decision to Examine

The examination of devices by the ABF is based on risk indicators determined by the examining officer at Ports of Entry (POE). Electronic devices are examined to determine whether they contain information relating to prohibited items, such as abhorrent and child exploitation material. Only trained ABF officers will undertake examinations of electronic devices.

The examination process involves the connection of the device to examination equipment and the review of the data stored on the device to determine a subsequent course of action.

There is no requirement for the traveller being present during an examination however the examination equipment is usually in a separate office and for operational and security reasons is not open to the public.

Officers may question travellers and examine goods if they suspect the person or goods may be of interest for immigration, customs, biosecurity, health, law-enforcement or national security reasons.

Passcode/Password

There is no legal compulsion for a traveller to provide a password/passcode or provide assistance to an electronic device at the border.

If an individual refuses to comply with a request or provide a password for an examination of their electronic device, and an ABF officer considers there to be a risk to the border, the ABF officer is authorised to seize that device for further examination prior to being returned.

None of the aforementioned legislation provide a time limit for the retention of goods subject to examination. Current ABF policy is to retain electronic devices held for examination for no longer than 14 days, unless it is reasonable that the examination will take longer or content is located on the device that renders the device subject to seizure.

Copy/Manipulate Data

Section 186A of the Customs Act allows, in certain circumstances, an officer of Customs to take copies of documents that have been examined. This includes copying data located on traveller's electronic devices. The circumstances are:

> as a result of that examination, an officer of Customs is satisfied that the document or part of the document may contain information relevant to:
>
> (i) an importation or exportation, or to a proposed importation or exportation, of prohibited goods; or
>
> (ii) the commission or attempted commission of any other offence against this Act or of any offence against a prescribed Act; or
>
> (iii) the performance of functions under section 17 of the *Australian Security Intelligence Organisation Act 1979*; or
>
> (iv) the performance of functions under section 6 of the *Intelligence Services Act 2001*; or
>
> (v) security (within the meaning of section 4 of the *Australian Security Intelligence Organisation Act 1979*);

Any copied information is stored securely and is subject to current ABF established security guidelines. The ABF does not alter or delete any data as a result of an examination of a device under the Customs or Migration acts.

Sharing Data

Copied data can only be shared depending on the type of information and the specific legislation that applies to that type of information, such as Part 6 of the *Australian Border Force Act, Privacy Act* or *Migration Act.* There are strict guidelines for the disclosure of such information.