**From:** Pavel Zakopaylo
**To:** Assistance Bill Consultation
**Subject:** Assistance and Access Bill 2018
**Date:** Monday, 10 September 2018 8:52:49 PM
**Attachments:** signature.asc

---

Dear Home Affairs,

I am an Australian citizen who is concerned about the powers given to law enforcement under the proposed Assistance and Access Bill. I believe the proposed expansion in search and surveillance capabilities further corrodes the already dwindling security and privacy of potentially innocent users.

My specific concerns, with reference to the explanatory document[0] provided by the Department of Home Affairs, are as follows:

(1) Schedule 3 seeks to expand the use of search warrants to allow law enforcement to remotely access a citizen's device, whereas before they needed to first be in physical possession of it.

Given that Android phones already have proprietary Google software running at the highest privilege level[1], this could (in combination with a Schedule 1 assistance notice) be used to silently deploy software to gather data about the user.

(2) Schedule 1 introduces mechanisms for law enforcement to request assistance from private companies, as opposed to simply requesting data. The scope of such assistance is sufficiently broad that the system needs more public oversight than what is provided in the bill.

Specifically, the transparency reports need to include what kind of data/assistance the reports asked for (and not simply the number of requests). Ultimately the line between providing access/assistance and introducing backdoors can be unclear, so public disclosure is required to ensure that the powers are being used fairly. (This includes the voluntary assistance requests; the pubic should know what kind of privacy/security guarantees they can expect from their communications providers.)

(3) I am also concerned about the increase in punishments for individuals that do not disclose decryption keys for their private devices. Search warrants can provide access to such devices, but that should only cover the data physically present on them.

The decrypted data is ultimately a combination of that data and a passphrase known by the owner; without this passphrase the decrypted data does not exist. Thus coercing an owner to produce a decryption key is equivalent to asking them to produce the data itself---i.e. to testify against themselves.

Thank you for your time.

Yours sincerely,
Pavel Zakopaylo

[0]
https://www.homeaffairs.gov.au/consultations/Documents/explanatory-document.pdf
[1] https://developers.google.com/android/guides/overview