Australia: Unprecedented surveillance bill rushed through parliament in 24 hours.

tutanota.com/blog/posts/australia-surveillance-bill

The Australian government has been moving towards a surveillance state for some years already. Now they are putting the nail in the coffin with an unprecedented surveillance bill that allows the police to hack your device, collect or delete your data, and take over your social media accounts; without sufficient safeguards to prevent abuse of these new powers.

This month the Australian government has passed a sweeping surveillance bill, worse than any similar legislation in any other five eye country.

The Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 gives the Australian Federal Police (AFP) and the Australian Criminal Intelligence Commission (ACIC) three new powers for dealing with online crime:

1. Data disruption warrant: gives the police the ability to "disrupt data" by modifying, copying, adding, or deleting it.

2. Network activity warrant: allows the police to collect intelligence from devices or networks that are used, or likely to be used, by those subject to the warrant

3. Account takeover warrant: allows the police to take control of an online account (e.g. social media) for the purposes of gathering information for an investigation.

The two Australian law enforcement bodies AFP and ACIC will soon have the power to modify, add, copy, or delete your data should you become a suspect in the investigation of a serious crime.

Amendments rushed through parliament

The Human Rights Law Centre criticizes that there are "insufficient safeguards" and that the government ignored "crucial recommendations of the bipartisan Parliamentary Joint Committee on Intelligence and Security that stronger safeguards are needed to protect the privacy of all Australians" while rushing the amendments through parliament on August 25th.

"It is alarming that, instead of accepting the Committee's recommendations and allowing time for scrutiny of subsequent amendments, the Morrison Government rushed these laws through Parliament in less than 24 hours."

What makes this legislation even worse is that there is no judicial oversight. A data disruption or network activity warrant could be issued by a member of the Administrative Appeals Tribunal, a warrant from a judge of a superior court is not needed.

Australian companies obliged to comply

When presented with such warrant from the Administrative Appeals Tribunal, Australian companies, system administrators etc. must comply, and actively help the police to modify, add, copy, or delete the data of a person under investigation. Refusing to comply could have one end up in jail for up to ten years, according to the new bill.

Required hacking activities could include: altering, copying and deleting data; intercepting and modifying communications; surveilling networks; and changing account credentials.

Justification of the bill

Politicians justify the need for the bill by stating that it is intended to fight child exploitation (CSAM) and terrorism. However, the bill itself enables law enforcement to investigate any "serious Commonwealth offence" or "serious State offence that has a federal aspect".

In fact, this wording enables the police to investigate any offence which is punishable by imprisonment of at least three years, including terrorism, sharing child abuse material, violence, acts of piracy, bankruptcy and company violations, and tax evasion.

Criticism of the surveillance bill

The Australian surveillance bill was heavily criticized by Senator Lidia Thorpe, the Greens spokesperson for Justice:

"The Richardson review concluded that this bill enables the AFP and ACIC to be 'judge, jury and executioner.' That's not how we deliver justice in this country. The bill does not identify or explain why these powers are necessary and our allies in the United States, the United Kingdom, Canada and New Zealand do not grant law enforcement these rights."

"In effect, this Bill would allow spy agencies to modify, copy, or delete your data with a data disruption warrant; collect intelligence on your online activities with a network activity warrant; also they can take over your social media and other online accounts and profiles with an account takeover warrant."

End of Human Rights

The new Australian surveillance bill signals the end of respect for Human Rights in Australia.

For lawyer Angus Murray, Chair of Electronic Frontiers Australia's Policy Team, the hacking powers pose a serious risk to our civil liberties.

"This is now a regime in Australia where we have conferred power on law enforcement agencies to hack Australians', and potentially overseas persons', computers and to take over accounts and modify and delete data on those accounts," he told Information Age.

"Australia doesn't have constitutionally enshrined rights to political speech and other human rights, but if we're going to give law enforcement these powers, that should be checked and balanced against a human rights instrument at Federal level."

Murray warns that there could come a point where this power is used against society. In theory, at least, the police could put something like child exploitation images onto your computer. While something like this is not the intention of the bill, there are also no significant safeguards against it.

Surveillance is power

Having the ability to secretly hack into people's computers, take over their social media channels, and spy on them fundamentally undermines our right to privacy.

Surveillance is power, and that is a threat to our free and open societies.

In Germany, we know from recent history how devastating a surveillance state is.

Together we must fight for privacy!