Australia flags tough new data protection laws this year

September 29 2022, by ROD McGUIRK

An Optus phone sign hangs above its store in Sydney, Australia, Thursday, Oct. 7, 2021. Australia's federal and state governments on Wednesday, Sept. 28, 2022, called for Optus to pay for replacing identification documents including passports and driver's licenses to avoid identity fraud after 9.8 million of the telecommunications company's customers had personal data stolen by computer hackers. Credit: AP Photo/Mark Baker, File

Australia could have tough new data protection laws in place this year in an urgent response to a cyberattack that stole from a telecommunications company the personal data of 9.8 million customers, the attorney-general said Thursday.

Attorney-General Mark Dreyfus said the government would make "urgent reforms" to the Privacy Act following the unprecedented hack last week on Optus, Australia's second-largest wireless carrier.

Dreyfus said "I think it's possible" for the law to be changed in the four remaining weeks that Parliament is scheduled to sit this year.

"I'm going to be looking very hard over the next four weeks at whether or not we can get reforms to the Privacy Act into the Parliament before the end of the year," Dreyfus told reporters. Parliament next sits on Oct. 25.

Dreyfus said penalties for failing to protect personal data had to be increased so that corporate boards could not dismiss fines as a "cost of doing business."

The "absolutely huge amounts" of customer data companies held for years would have to be justified under the amended law, Dreyfus said.

"Companies need to look at data storage not as an asset, but as a liability or a potential liability," Dreyfus said. "For too long we have had companies solely looking at data as an asset that they can use commercially."

The government blames lax cybersecurity at Optus, a subsidiary of Singapore Telecommunications Ltd., also known as Singtel, for the theft of current and former customers' personal information.

Singtel apologized in a statement issued Wednesday by its management saying, "We are deeply sorry to everyone affected by the data theft."

"Since the incident, our focus has been on supporting Optus' efforts to help impacted customers and strengthen their security controls," the statement said.

"Information security is of paramount importance to the Singtel Group and a top priority across all of its business units and we invest significant resources to continually strengthen our defenses against emerging threats," the statement added.

The data included passport, driver's license and national health care identification numbers which could be used for identity theft and fraud.

Authorities are critical of Optus' initial failure to disclose that Medicare numbers were among the stolen data. That became apparent Tuesday when the hacker dumped the records of 10,000 customers on the dark web—six days after Optus discovered the cyberattack.

The urgent legislative response is separate from a broader review of the Privacy Act that began three years ago. The law was passed in 1988 and critics argue it badly needs to be adapted to the digital age.

Optus could potentially be fined a maximum 2 million Australian dollars ($1.3 million) for breaching the Privacy Act, the government said.

It could be fined hundreds of millions of dollars over a similar security breach under European Union laws, the government said.

Submissions to the Privacy Act review have suggested penalties for breaches equivalent to 10% of revenue from Australian operations.

Optus CEO Kelly Bayer Rosmarin has argued against increased fines, telling the Australian Broadcasting Corp. on Tuesday: "Honestly, I'm not sure what penalties benefit anybody."

Optus maintains it was the target of a sophisticated cyberattack that penetrated several layers of security.

After an emergency meeting with banking and consumer regulators, Financial Services Minister Stephen Jones said "fraudsters" and "scammers" were already beginning to use the stolen data, which includes phone numbers and email addresses.

With personal information stolen from 38% of Australia's population of 26 million in the hack, "you can't overestimate the impact of this breach on consumer issues," Jones said.

He warned compromised Optus customers against activating URLs they receive by text or email because they could be from criminals attempting to steal more information.

"We're all working as best as we can to try and work our way through the long tail of problems that is going to be a consequence of this massive data breach," Jones said.