Australia: Massive Optus data breach highlights lax regulations for telco giants

Oscar Grenfell
4 October 2022

Over the past fortnight, millions of people have faced a great deal of uncertainty after it was revealed that Optus, one of Australia's largest telecommunications providers, had been hit by a successful hack.

Ever since it announced the breach, the corporation has engaged in a damage control exercise aimed at minimising its liability. Information about the hack has been drip fed to customers and the population, meaning that much remains unknown about the nature of the hack and the extent of the material that has been compromised.

What is known, however, is highly concerning. On Monday, a week-and-a-half after the breach was reported, Optus revealed that the personal identification details of more than two million customers had been breached. The expired details of another 900,000 people were also hacked.

The night before, Optus had sent text messages and emails to some current and former customers, indicating that they had been impacted by the breach.

The belated character of Optus's announcements means there is every possibility that the details of all ten million of its customers may be caught up in the hack. That would amount to almost 40 percent of the population.

The information that has been hacked includes passport and driver's licence details, as well as Medicare and other social security information. Email addresses, full names, dates of birth and even residential statuses are in the data that has been pilfered.

Experts have warned that those affected could be victimised by a range of different type of fraud. At the low end, this could include increased phishing attacks, involving emails and texts containing harmful links aimed at stealing further details. At the high end, some people could be targeted for identity theft, as well as the opening of fraudulent bank and mobile phone accounts.

Already, the details of some 10,000 Optus users have been posted to an online forum. The information of other customers could be being traded on the black market.

The company's response has prompted widespread anger. Optus customers have complained on social media over the delayed and uninformative communications from the corporation.

Many are unclear about whether they need to engage in the onerous, time-consuming process of changing their drivers' licence numbers and passport details to protect themselves. Optus has given undertakings to pay the related fees for those who are affected. In a number of states, however, the exact processes by which this will occur, and which customers will be eligible, remain vague.

More broadly, the hack has pointed to the dangerous consequences of for-profit corporations controlling vast swathes of data, and a key social utility, i.e., telecommunications. There is a clear conflict between the privacy interests of ordinary people and the commercial impulses of such companies to retain as much data as possible, while seeking to minimise the costs required to protect it.

At the same time, ever-greater government surveillance imposes requirements on such corporations to retain information for extended periods, even if it is not needed for the service requirements of customers.

When it reported the breach, Optus claimed that it had been the victim of a "sophisticated" hack. That assertion has been rejected by the federal Labor government, the country's digital security agencies and independent experts.

The Information Security Media Group (ISMG), an intelligence firm, reported early last week that the hacker had taken the data by accessing an unsecured Application Programming Interface (API)—software that is used to share data between computer programs and devices.

This was later confirmed to ISMG by the hackers. Calling themselves "Optusdata," they wrote in a message:

"No authenticate needed. That is bad access control. All open to internet for any one to use." In other words, the information was connected to the Internet and was not protected in any way.

Other aspects of the hack have led cybersecurity experts to speculate that "Optusdata" is not a sophisticated hacking organisation. It demanded a payment from Optus of $AU1.5 million in return for the data, an unusually low sum. It later posted messages to an online forum in childish English, apologising for the inconvenience caused by the hack and expressing contrition.

If the data breach had occurred in Europe or the United States, Optus would be liable for government-imposed financial penalties that could reach hundreds of millions of dollars.

In Australia, there is no such liability. Under the legislation that governs data protection in the sector, penalties for company violations of general security provisions are capped at $250,000 per infringement. Fines for corporations that breach privacy obligations are capped at $2.2 million.

Prior to the hack, there had been plans for Optus to be floated on the Australian Stock Exchange. Estimates of its valuation had ranged from eight to twelve billion Australian dollars. Optus has an operating revenue of over $7 billion. Singtel, Optus' parent company, reported a net profit of $1.95 billion in the last financial year.

The extent of the Optus leak has resulted in a substantial degree of publicity, but there is every indication that massive data breaches are occurring frequently, with the corporations involved facing minimal consequences.

The *Australian Financial Review* reported yesterday that freedom of information requests to the Office of the Australian Information Commissioner (OAIC) revealed at least 11 such breaches in the first six months of the year, each of them affecting 10,000 or more customers.

A report on the *Pearls and Irritations* website cited a 2019 report by the OAIC, also obtained under freedom of information laws. It stated that "overall, the response system [to data breaches] is either non-existent or performing poorly from a citizen's perspective." The report "observed significant deficiencies in response standards, formal reporting channels of Government, and meaningful protection for consumers."

While successive governments have presided over a lax regulatory framework, they have increased requirements for corporations to retain data, in line with a broader surveillance regime.

Australian legislation, bolstered in 2015, requires companies to retain all data they acquire, through the life of a contract and for two years afterward. Justified on the basis of combating terrorism and serious crime, the draconian data retention framework is part of a broader onslaught on democratic rights, with intelligence and other government agencies granted ever-expanding powers to spy on the private information and communications of citizens. The real target is mounting social and political opposition within the working class.

The Labor government has demagogically condemned Optus and adopted a pose of frustration with its response, but Labor, no less than the Liberal-National Coalition, is responsible for both the lax regulatory framework that imposes virtually no penalties for such breaches, and the intrusive data retention requirements.

Prominent legal firms are floating the possibility of class actions, which, given the number of customers affected, could be among the largest in history. Government officials are also flagging possible, as yet unspecified, regulatory changes.

Whatever these outcomes, however, the Optus saga highlights the incompatibility between the needs and interests of ordinary people in a complex modern society, and the domination of critical infrastructure by vast corporations whose only motive is to maximize profits and shareholder returns. It is another reason to place telecommunications, along with the banks and big business, under public ownership and the democratic control of the working class, as part of a broader socialist transformation of society.