Dated and Fractured: Optus and Data Protections Down Under

By Dr. Binoy Kampmark
Asia-Pacific Research, October 03, 2022

Region: Oceania
Theme: Defence

***

Things are not getting better for Optus, a subsidiary of the Singapore-owned Singtel and Australia's second largest telecommunications company. Responsible for one of Australia's largest data breaches, the beleaguered company is facing burning accusations and questions on various fronts. It is also proving to be rather less than forthcoming about details as to what has been compromised in the leak.

First, for the claimed story, which has been, at points, vague. On September 22, the telecommunications company revealed that details of up to 9.8 million customers had been stolen from their database. Dating back to 2017, these include names, birthdates, phone numbers, email addresses and, in a number of cases, addresses, passport number or driver's licenses.

Fittingly, and perversely, a study from the Australian Institute of Criminology that same year found that one in four Australians had been victims of identity crime or a general misuse of personal information. A less than comforting observation from the authors was the remark that such rates were "comparable with the 27 percent reported by respondents to the identity fraud survey conducted in 2012 for the United Kingdom's National Fraud Authority".

In the case of Optus, the company claims that the breach arose from a "sophisticated cyberattack". The view from those outside Optus is somewhat different. The attack

seemed to have occurred when an application programming interface (API) was linked to an Optus customer database leaving it easily accessible. In basic terms, an API permits the transfer of data. Left naked and vulnerable, users can merrily pry their way into systems they would otherwise not have access to.

The almost tearful defence of the breach offered by Optus CEO Kelly Bayer Rosmarin was decidedly unimpressive, despite some prattling in the press about "a courageous and correct call to get in front of the media in a video call that felt strangely intimate and completely open". During a streaky display, she claimed that "we are not the villains" and suggested that the API was not freely exposed.

Bayer Rosmarin, however, is defending a crumbling front, made almost absurdly stark by her unimpressively light burden of responsibilities. Among them, making Australia's recently retired tennis star, Ash Barty, the company's Chief Inspiration Officer, and Australian Formula One racer Daniel Ricciardo Optus Chief Optimism Officer, have been foremost.

Less laughable is the general dislike for regulatory oversight in data security exhibited by a whole spectrum of Australian companies. As Tom Burton from the *Australian Financial Review* sniffily remarks, "intense lobbying from financial, payment, telco, media and marketing interests" retarded reforms towards "a trusted, secure, reliable and efficient regulatory regime to manage the burgeoning digital economy and the data that fuels it." As a feature of this reluctance, Australian banks muttered and grumbled when asked to confirm bank account holder details linked to the account prior to making payments.

Those found wounded and floundering in terms of identity breaches have had little by way of remedial recourse. Australians, almost uniquely in the Anglo family of smug self-praise, have no self-standing right to sue for the civil wrong of a breach in privacy. The Australian common law remains perversely stubborn in articulating a clear tort on the subject, and legislators have been less than swift in moving matters into legislation.

The *Privacy Act 1988* (Cth), given its numerous exemptions for small businesses, employee records, media bodies and political parties, is but a poor, shabby cover. It certainly falls far short of its European cousin many times removed, the General Data Protection Regulation (GDPR).

In a 2019 report released by the Department of Home Affairs under Freedom of Information, David Lacey and Roger Wilkins, a former secretary of the Attorney-General's Department, found that "overall, the response system [to data breaches] is either non-existent or performing poorly from a citizen's perspective." The authors "observed significant deficiencies in response standards, formal reporting channels of Government, and meaningful protection for consumers."

The condition was made egregiously worse by Australian legislation mandating the retention of customer data for up to two years, though there is no strict requirement *not* to keep such data after that period. The Department of Home Affairs states that such a policy ensures "Australia's law enforcement and security agencies are lawfully able to access data, subject to strict controls."

The Telecommunications Consumer Protections Code, overseen by the Australian Communications and Media Authority, also permits telcos to hold personal data for billing

information purposes “up to six years prior to the date the information is requested”. This does not, however, necessitate the retention of passport details, drivers’ licenses and Medicare numbers.

The implication of such provisions is unmistakable. They have encouraged companies to engage in a course of conduct that has made security feeble and breaches likely. They have become the shoddy handmaidens of government paranoia.

Entities such as Optus simply cannot be seen to be reliable in responding to such crises. The sombre assessment from digital rights advocate Lizzie O’Shea is dire. “My third law of IT is that every time there is a data breach, one of the first lines out of the spokesperson’s mouth is that they take security seriously – even if they have demonstrably proven they are not.” While accepting the obvious point that Optus is not directly responsible for the conduct, she stingingly suggests that “you can’t complain that something’s been stolen when you haven’t locked the front door.”

The policy implications are vast. Should such telcos be required to hold data as required under problematic data retention law that has been assailed in the EU? (In September, Germany’s general data retention law was found by the European Court of Justice to violate EU law.) Making such organisations holders of such information renders them rich targets.

Penalties have been proposed. In the context of the European Union and California, stiff monetary sanctions apply, a point Home Affairs Minister Clare O’Neil has noted. Current fines in the order of A$2.2 million for companies and A$440,000 for individuals are risible. There are promises from Optus to fork out to replace compromised documents. But in terms of legislative protections, Australian policy makers continue to look at data protection through a lens fractured and dated.

*

Note to readers: Please click the share buttons above or below. Follow us on Instagram and Twitter and subscribe to our Telegram Channel. Feel free to repost and share widely Global Research articles.

Dr. Binoy Kampmark *was a Commonwealth Scholar at Selwyn College, Cambridge. He currently lectures at RMIT University. He is a regular contributor to Global Research and Asia-Pacific Research. Email: bkampmark@gmail.com*

Featured image: Optus’ Queensland head office, in Fortitude Valley (Photo by Kgbo, licensed under CC BY-SA 4.0)

Articles by: **Dr. Binoy Kampmark**