OpenVoiceNews Australia

Transparent. Unbiased. Yours.

Empowering Australians to Demand Deletion of Their Personal Data Could Curb Mass Cyber Theft

July 17, 2025

— Categories: General News

Allowing Australians the legal right to force companies to erase their data from databases could be a vital step in fighting the rising tide of mass data breaches, cybersecurity experts argue. Recent attacks on major firms like Qantas Airways, Optus, and Medibank have exposed sensitive information of over 25 million Australians, highlighting the urgent need for stronger personal data protections.

Ryan Ko, a cybersecurity professor at the University of Queensland (UQ), warns that the threat from cybercriminal groups is growing daily. These criminals often exploit vulnerabilities in company systems to steal data for identity theft, extortion, or worse. "There's no way you can tell how the leaked information is going to be used," Ko explains. "You're just a sitting duck." He advocates for a "right to erasure" policy, which would allow individuals to hold companies accountable by demanding the deletion or anonymization of their personal information.

Ko points to the organized nature of these cybercriminal gangs, some of which are even state-sponsored, that take advantage of weaknesses in Australia's corporate cybersecurity frameworks. Despite a Harvard University report in 2022 ranking Australia as the global leader in cyber defense, many companies still lack the governance and resilience needed to prevent large-scale breaches.

The massive Optus hack in September 2022 revealed personal details, including names, birthdates, addresses, and passport numbers, of nearly 9.8 million customers. Queensland alone had to replace over 178,000 driver's licenses due to the breach. Attackers exploited flaws such as unsecured application programming interfaces (APIs). The following month, Medibank suffered a ransomware attack, compromising the medical records of 9.7 million people. Hackers allegedly used stolen credentials from an employee's private computer to access sensitive systems, exposing Medibank's insufficient security measures, like the absence of multi-factor authentication and delayed responses to consultant warnings.

Qantas also experienced a significant breach in late 2023 when hackers accessed the personal information of 5.7 million Frequent Flyer members via the airline's call center in the Philippines. Among those affected was a federal Member of Parliament who publicly criticized Qantas for its lack of transparency regarding the extent of the data accessed. Qantas has since sought legal injunctions to prevent the misuse or public dissemination of the stolen data, but the full consequences remain uncertain.

Regulatory investigations into these breaches continue to drag on. The Office of the Australian Information Commissioner (OAIC) is still probing the Optus attack nearly three years later, while the Australian Communications and Media Authority (ACMA) has sued Optus ithe n the Federal Court. Similarly, OAIC's legal action against Medibank remains active alongside multiple class-action lawsuits from affected customers.

In response to these breaches, the federal government introduced privacy reforms in December 2022, strengthening the OAIC's powers to impose penalties, raising maximum fines from $2.2 million to $50 million for serious breaches. Still, experts say these regulatory changes alone are not enough.

Katharine Kemp, a privacy scholar at the University of New South Wales, critiques companies for exploiting vague data guidelines to hoard and monetize customer information. She supports implementing the "right to erasure," a policy already established in Europe since 2018, which would empower individuals to demand transparency and deletion of their data. According to a 2023 OAIC survey of 1,600 Australians, 90% support this right, reflecting widespread public concern over data privacy.

Given the slow pace of government investigations and the increasing scale of cyber threats, introducing a legally enforceable right to erase personal data could provide Australians with a critical tool to reclaim control over their information and reduce the impact of future cyberattacks.