Australia and New Zealand's New Privacy Laws and Enforcement Measures in an Era of Digital Growth

Brian Daigle and Mahnaz Khan, Office of Industries
brian.daigle@usitc.gov; mahnaz.khan@usitc.gov

Australia and New Zealand have had privacy principles embedded in their laws since the 1980/90s, long before the Internet boom. After the European Union's 2016 General Data Protection Regulation (GDPR) was implemented in 2018, many countries such as Australia and New Zealand drafted legislation to update their privacy and data protection laws so that their digital economies could participate in the EU and other global digital markets. This EBOT examines both Australia's and New Zealand's privacy laws and contrasts these laws to standards set by GDPR, in addition to analyzing the two countries' enforcement practices.[1] New Zealand's enforcement has been limited. By contrast, two recent enforcement actions by Australia against U.S. tech firms highlight the growing importance of these regulations on digital trade.

Australia and New Zealand's Digital Trade Economies are Booming

As the world becomes more digitally connected, digital trade has been increasingly important to Australia's and New Zealand's growing economies. According to latest figures posted by the Export Council of Australia, the country's digital trade economy was valued at $33 billion, with digital trade exports valued at $4.6 billion in 2017. New Zealand's digital trade data is not publicly reported, but one report estimated that IT-related service exports in the New Zealand were $1.1 billion in 2020. According to the World Bank, Australia's information and communication technology (ICT) service exports, a subset of digital trade exports, grew more rapidly at 75 percent compared to New Zealand's 27 percent growth from 2010-2017.[2]

Australia and New Zealand Have Recently Adopted Privacy Laws in Line with the GDPR

The foundation of Australia's and New Zealand's privacy laws are based on the OECD's Guidelines for Privacy, which were introduced in 1980. Like many other countries, Australia and New Zealand have both changed or are in the process of changing their country's privacy laws for their growing digital economies in order to reflect some of the elements in the EU's GDPR. One of the impetus for the change in their countries' privacy laws is to allow Australia and New Zealand to continue participating in the global digital economy vis-à-vis the EU market. Under GDPR, the EU makes adequacy determination that a third-party country offers the similar level of protection as the GDPR, which would permits a cross-border transfers in and out of the EU to the third-party country without authorization from an EU national supervisory authority.

Industry sources observe that New Zealand's privacy framework more closely mirrors the GDPR than Australia's. New Zealand passed its Privacy Law Act 2020 in December 2020, replacing its Privacy Bill 1993. In 2018, the EU made an adequacy determination that New Zealand's Privacy Bill 1993 offers the same level of protections as the GDPR because it was a strong privacy regime that gave citizens access to their personal data; however, the EU decided that New Zealand's laws were due for a reevaluation of adequacy in 2020. The reevaluation was the impetus for New Zealand to change its privacy laws in 2020 to account for breach notification requirements, stronger enforcement mechanisms with criminal penalties, and strengthening cross-border data protections, thereby aligning their privacy regime closely with the GDPR.

[1] A discussion of the EU's enforcement of GDPR can be found at Daigle, Brian and Mahnaz Khan, "The EU General Data Protection Regulation, An Analysis of Enforcement Trends," June 2020.

[2] The World Bank defines information and communication technology service exports (ICT service exports) as including computer and communications services (telecommunications and postal and courier services) and information services (computer data and news-related service transactions).

However, New Zealand chose not to align their privacy regulations with other elements of GDPR, such as the "right to be forgotten," "data portability," or the larger fines for noncompliance that GDPR features.[3]

Australia has not yet adopted a standalone privacy act to cover online data, despite being a larger digital economy than New Zealand. Australia's existing Privacy Act has been revised three times since its inception in 1980 (most recently in 2018), and the country is expected to enact new privacy laws in 2021. Industry sources contend that Australia's new privacy framework will be modeled mainly on GDPR but will not be as extensive or as strict as GDPR. Currently, one key difference being discussed by Australian government regulators is that Australia may recognize that businesses are able to obtain consent to process personal data online through either implied or express consent, whereas GDPR specifically only permits express consent. In addition, Australia's 2018 amendments, which mainly targeted breach notifications, differed from GDPR by adopting a 30-day timeframe for which serious data breaches needed to be reported, in sharp contrast to GDPR's requirement that a data breach be reported within 72 hours.

Additionally, the structure for fines for non-compliance also differs between the two jurisdictions and from GDPR. Both New Zealand and Australia's fines are substantially lower than fines under GDPR, which can reach up to €20 million (U.S. $24 million) or 4 percent of a company's gross revenue. The highest fine for a single privacy violation that can be issued in New Zealand is only NZD$10,000 (U.S. $7,141), in contrast to Australia's much higher limit of AUS$2.1 million (U.S. $1.6 million) per violation.

Two U.S. Firms are the Subject of Recent Enforcement Actions from Australia

Historically, New Zealand has not brought significant enforcement actions under its privacy regulations, in contrast to Australia, which has shown increased interest in privacy enforcement. This includes two ongoing cases from 2020 involving large U.S. tech firms; in March 2020, the Australian Information Commissioner sued Facebook for breaching the privacy law in its disclosure of over 300,000 Australian users' information in the "This Is Your Digital Life" survey product. Though the case has not yet been decided, Facebook may face a fine of up to AUS$529 billion (U.S. $404 billion) if it is found to be in breach of Australian data privacy regulations. For enforcement purposes, Australian regulators consider Facebook to have committed 300,000 individual data breaches, with each users' data breach representing an individual violation of AUS$2.1 million maximum fine per violation.

In July 2020, the Australian Competition and Consumer Commission (ACC) also filed a lawsuit against Google for allegations that it violated privacy and consent obligations. The ACC claims that Google did not effectively gather consent from Australian users when it expanded the collection of personal information for its targeted advertising program.

Sources: Australian Government, Department of Foreign Affairs and Trade, "*Digital Trade and the Digital Economy*," (accessed April 14, 2021); World Bank, *Balance of Payments Statistics Yearbook* (accessed April 8, 2021); Jonathan Miller and Hamish Grant, *Valuing the Digital Economy of New Zealand*, Asia Pacific Sustainable Journal, Vol. 26, No. 1; Australian Government, Office of the Information Commissioner, *Australian Entities and the EU General Data Protection Regulation (GDPR),* June 8, 2018; Reuters, "Australia Sues Facebook, Alleges Breach of User Data," March 9, 2020; The Guardian, "ACCC Sues Google for Collecting Australian Users' Data Without Informed Consent," July 27, 2020.

[3] The "right to be forgotten" refers to the concept that individuals have the right to ask organizations to delete their personal data. "Data portability" is the concept that allows data subjects to obtain data that a data controller holds on them and to reuse it for their own purposes. Individuals are free to either store the data for personal use or to transmit it to another data controller.