Data privacy: Stricter European rules will have repercussions in Australia as global divisions grow

July 31 2020, by Normann Witzleb

Credit: AI-generated image (disclaimer)

A big year for privacy just got bigger. On July 16, Europe's top court ruled on the legality of two mechanisms for cross-border transfers of personal data.

The Court of Justice of the European Union (CJEU) struck down the "EU-US Privacy Shield", an intergovernmental agreement on which thousands of US companies based their data processing with EU trading partners and consumers. At the same time, the CJEU generally upheld so-called "standard contractual clauses" (SCC) for data exports but imposed new requirements on their use.

The decision has an immediate impact on data flows between the U.S. and the EU. But it will also create new challenges for Australian companies that engage with Europe.

The global reach of European privacy laws

In 2018, the EU brought into force the General Data Protection Regulation (GDPR), one of the world's strongest privacy protection frameworks. This latest decision provides further evidence that the GDPR has impact far beyond the EU. It allows data about European citizens to be exported outside the bloc only if an adequate level of data protection is guaranteed.

Adequacy can be demonstrated at country level, and some major trading partners of the EU (such as Japan, Canada and New Zealand) have been certified by the EU as having a comparable level of privacy protection. Until a fortnight ago, US companies could likewise rely on an adequacy decision for the EU-US Privacy Shield. The Privacy Shield allowed companies to self-certify their data practices against a set of minimum criteria and enhanced US regulatory oversight. The Court has now held that this is not enough.

What does this mean for Australia?

Australian companies and consumers need to be mindful of the new

CJEU decision. Data exports are very common, particularly where companies operate multi-nationally, outsource some of their data processing or store data on overseas cloud servers.

Australia was not a party to the EU-US Privacy Shield. It also does not have EU adequacy status. This is because our Privacy Act does not apply to small businesses, employee data, and political parties, amongst others. An EU entity that seeks to export personal data to Australia therefore needs to use other safeguards to ensure that EU personal data remains protected.

This is commonly done in the form of standard contractual clauses, by which the sender and recipient of data agree that their data processing meets GDPR standards. The CJEU has now clarified that companies and regulators must verify in each case that the clauses stand up in light of the recipient country's data laws.

Governmental surveillance programs and access to effective legal remedies are a particular concern. Privacy professionals around the world now have to work out what this new requirement means.

Deepening global divisions and the trend to data localisation

To comply with the ruling, companies need to engage in a more detailed risk analysis than before. In some cases, data may no longer be transferred. This is likely to contribute to an international trend to house critical data locally. A recent example of this trend is the COVIDSafe app: the data it collects must remain in Australia.

The CJEU decision comes at a time of intense public debate of privacy in Australia and many other countries. The COVID-19 pandemic has

turbo-charged the digitalisation of many aspects of daily life. Every digital transaction leaves traces in the form of personal information, which could be a target for data mining and surveillance by corporate and state actors.

It would be sensible to adopt internationally harmonized data protection standards to regulate global data streams. But the world appears currently headed in the opposite direction.

Despite both the EU and US sides emphasizing the need for cooperation after the CJEU ruling, the major trading powers and blocs are increasingly pitted against each other.

Apart from the long-standing EU-US division over privacy, China, India and Russia have also begun to assert their own distinct data processing models. These powers generally give their citizens fewer privacy rights than the EU. They also make increasing use of data localisation requirements, which prohibit or impede data export, to enforce their own data protection protocols. The intensifying conflict between the US and China, most recently erupting over the new security laws for Hong Kong, also marks data governance and cybersecurity as significant battlegrounds.

Australia's new challenges in data protection

Australia's data regulation tends to be pragmatic and business-friendly. It steers a middle course between the conflicting privacy approaches of the US and the EU. However, in a world retreating from globalized regulation, it is becoming increasingly difficult not to take sides.

Privacy is looming larger than ever in public consciousness, and Australia's Privacy Act is due for an overhaul. More than ever, Australia needs to determine its own course in safeguarding personal information

against potential overreach by corporations and governments.