Australian Information and Privacy Commissioner Angelene Falk to Propose Global Policy on Mandatory Notification of Data Breaches

We continue our ongoing interview series 'Commissioners Around the World' with a conversation with Angelene Falk, the Australian Information Commissioner and Privacy Commissioner and Executive Committee member of the International Conference of Data Protection and Privacy Commissioners (ICDPPC). As we count down to the next annual ICDPPC meeting in Tirana this October, the Executive Editor of the European Data Protection Law Review (EDPL), Nelly Stratieva, is speaking to national data protection regulators about the latest from their part of the world and their expectations about international cooperation.

In this interview, Australian Commissioner Falk discusses her country's new Consumer Data Right and Digital Platforms Inquiry, as well as the recently introduced mandatory notification of data breaches. Commissioner Falk points out the need for greater interoperability between regional frameworks in light of their growing number across the globe. She proposes a concrete step in that direction – the adoption of a resolution at the upcoming 41st ICDPPC for a global policy on mandatory notification of data breaches.

NS: Could you tell our readers more about the current privacy and data protection issues and initiatives in Australia?

AF: As Australia's national privacy regulator, I am involved in a number of initiatives aimed at effectively regulating privacy in the digital age. One of the key regulatory themes we are pursuing is how to get the right balance between privacy self-management and organisational accountability. We are holding organisations to account and working to support consumers in making informed decisions about their personal information.

One of the major changes over the coming months will be the new Australian Consumer Data Right, or CDR. This is a data portability measure intended to create more competition and choice in the market by giving consumers control over how their data is used and disclosed.

It will allow consumers to access particular data in a readily usable form and direct a business to securely transfer it to another accredited business. My role is to ensure that strong privacy safeguards are built into the system, so consumers can benefit from being able to switch service providers while their personal information is protected. We will also resolve consumer complaints from individuals and small businesses, once the system is operational in February 2020.

Another important area of focus is the way digital platforms are handling personal information. Our competition regulator in Australia, the Australian Competition and Consumer Commission (ACCC), has just completed an inquiry into the effect that digital search engines, social media platforms and other digital content aggregation platforms are having on competition in media and advertising service markets.

The inquiry has also looked at whether existing regulatory frameworks for the collection and use of data remain effective in addressing the challenges of digitisation and the world of targeted advertising. We have been collaborating with the ACCC to consider ways to strengthen data protection outcomes for Australians, and this process has recommended reforms to our privacy laws to ensure that our framework is meeting the evolving challenges we face in this digital environment.

In both these areas — the Consumer Data Right and the Digital Platforms Inquiry — we have been working closely with the Australian competition regulator. This collaboration between data protection and consumer protection authorities is an essential part of protecting consumers in the digital age. This was also recognised by the ICDPPC's 39th conference, in Hong Kong in 2017, when it adopted a resolution on collaboration between data protection authorities and consumer protection authorities for better protection of citizens and consumers in the digital economy.

In 2018, Australia introduced mandatory notification of data breaches to affected consumers and the privacy regulator. This means that where someone's privacy has been breached, and they are at risk of serious harm, they are informed of that breach and are able to take the necessary steps to protect their personal information. Our regulatory focus during the first year of the Notifiable Data Breaches scheme has been on driving awareness of entities' obligations and of the causes of data breaches to support better practices. Many entities have taken a proactive approach to engaging with us, allowing us to work constructively with them to ensure an effective response. To date, we have clearly seen how the scheme is increasing transparency and accountability for personal information handling practices.

Mandatory notification of data breaches is a feature of many data protection frameworks around the globe, and I will be presenting a proposed resolution in Tirana that contributes to a global ICDPPC policy on this issue, with the goal of preventing personal data breaches through security safeguards that target the 'human factor'.

NS: The GDPR resounded around Europe and the world. In your opinion, what will be the next legislative frontier that could have such disruptive power?

AF: The GDPR has had a big impact on information handling around the world, and it continues to influence data protection legislation in other jurisdictions.

In today's digital age we need our legal frameworks to reflect technological developments so they remain fit for purpose. I expect we will continue to see legislative changes in the years to come. To succeed, they will need to provide for greater interoperability between regional frameworks.

Interoperability doesn't mean uniformity, but instead recognises the differences in our frameworks and provides a bridge to ensure that personal information is protected no matter where it flows. As regulators, we can work towards this by collaborating on developing policy positions, guidance, tools and enforcement.

These efforts are already reflected in the standards we are seeing emerge around the world: the GDPR, Convention 108, the Ibero American Data Protection Standards, APEC Cross Border Privacy Rules (CBPR) and the OECD Privacy Guidelines. International data transfers can also be facilitated through other regulatory tools such as certification and privacy seals, codes of conduct, binding corporate rules and standard contractual clauses, to name a few.

Building on this, we are considering the role a certification scheme could play in Australia as a way for organisations to demonstrate their accountability in personal information handling. We are looking at what's been done on this already in jurisdictions like the EU, Japan, and Singapore.

We are also implementing the APEC Cross Border Privacy Rules in Australia, which my office will enforce. In doing this we can learn from others further down the CBPR road, like the US, Japan and Singapore, where this mechanism is in place to provide accountable cross-border data transfers.

As a regulator, my ability to efficiently prevent, detect, deter and remedy relies on cooperation and collaboration, and a framework that is interoperable with other regions.

NS: What major issues do you hope will be addressed at the 41st ICDPPC in Tirana? Which topics are of most importance for you?

AF: The themes of this year's conference – convergence and connectivity – could not be more relevant in 2019. Around the world we are seeing data protection laws intersect with consumer protection, human rights and the digital economy.

This convergence underlines the importance of collaboration between privacy regulators. Collaboration between data protection authorities and consumer protection authorities is also an essential part of protecting consumers in the digital economy. In Australia, this is borne out in our work with the Australian Competition and Consumer Commission on a range of initiatives including the Australian Consumer Data Right and an inquiry into digital platforms. My office also co-chairs the ICDPPC's Digital Citizen and Consumer Working Group with the Office of the Privacy Commissioner of Canada.

Accountability is the other important topic I see at this year's conference. The interrelationship between privacy self-management and organisational accountability is crucial to raising global data protection standards in the digital age. Done well, privacy self-management allows individuals to exercise choice and control by understanding how their personal information is being handled. But it's reliant on organisations making this information accessible and understandable, and we must continue our focus in this regard.