University of New South Wales Law Research Series

EVALUATING GDPR: GLOBAL IMPACT ON SURVEILLANCE PRACTICES (A CONTRIBUTION TO THE IAPP'S 'THE GDPR AT TWO: EXPERT PERSPECTIVES' SERIES)

GRAHAM GREENLEAF

(Contribution to 'The GDPR at Two: Expert Perspectives' Series, 28 May 2020)
[2020] *UNSWLRS* 35

UNSW Law
UNSW Sydney NSW 2052 Australia

E: unswlrs@unsw.edu.au
W: http://www.law.unsw.edu.au/research/faculty-publications
AustLII: http://www.austlii.edu.au/au/journals/UNSWLRS/
SSRN: http://www.ssrn.com/link/UNSW-LEG.html

Evaluating GDPR: Global impact on surveillance practices

(A contribution to the iapp's 'The GDPR at Two: Expert Perspectives' series)

The International Association of Privacy Professionals (iapp) commissioned eleven short assessments of the GDPR for its second anniversary, 28 May 2020, of which this is one.

Graham Greenleaf, Professor of Law & Information Systems, University of New South Wales

An evaluation of the GDPR's first two years depends upon how you measure 'success', which means you must ask what you hope it can achieve. I want the GDPR to make a substantial contribution to the dismantling of surveillance capitalism, and its replacement by a less dangerous information-based capitalism. A European data privacy law cannot achieve this goal by itself, no matter how strong its principles or its enforcement. Fundamental changes to the business models of surveillance capitalism will at least require the parallel efforts of EU competition, consumer protection and anti-discrimination laws and regulators. It will also require complementary contributions by data privacy and other regulators and laws globally, not least in the USA which is the home and 'safe harbor' of the inventors and key proponents of its practices. Seen from this perspective, how does the GDPR shape up as a two-year-old toddler?

The GDPR's first great success has been as a global inspiration for legislation which borrows from its principles and enforcement mechanisms. For 50 years since Hesse's *Datenschutzgesetz* of 1970, countries have been slowly enacting, and even more slowly enforcing, data privacy laws. As of December 2019, 142 countries have done so. These laws are of greatly varying quality, but overwhelmingly influenced by the European model of data privacy laws. Since 2016 new laws outside Europe have included hundreds of examples of GDPR-inspired principles or enforcement mechanisms. In Asia alone, new laws in Thailand and Korea and bills in India, Indonesia and Sri Lanka are creating a new post-GDPR momentum. In Africa, 14 countries have new laws since 2014. The new global template is becoming a version of the GDPR.

Competitors for global influence are unimpressive. APEC-CBPRs, designed to hoover the world's personal data into the USA, is deservedly dead: only 28 US companies and 3 Japanese companies, and no others, participate after a decade. The OECD privacy Guidelines are stuck in 1980, unwilling to go forward.

Within the EU, administrative fines necessarily move slowly through the GDPR systems, due to rights of appeal and the consistency mechanism's collaboration requirements among DPAs. So far, the highest proposed fines (not yet finalised) only amount to less than US$250 million (British Airways), but they are capable of being in the billions, and need to be. Meanwhile, lesser fines establish precedents for breaches of key GDPR provisions, such as Google's US$8 million fine by Sweden's DPA for delisting (RTBF) breaches. Enforcement actions initiated by data subjects or their representatives are well-supported and required by the GDPR (art. 80). Many of the most significant GDPR enforcement actions have been at the initiative of 'privacy NGOs' (such as NOYB and LQDN). So far, NGO-supported actions have focussed on obtaining corrective actions and administrative fines, but they will soon also include large-scale actions for compensation (art. 82). Depending on national laws, class actions involving commercial lawyers will also emerge. Shutting down infringing types of processing will depend on national laws (art. 84). The GDPR has all the tools to create a market for privacy enforcement, a level of 'responsive regulation' Europe has not previously seen. Will EU regulators be willing to use them to their full 'dissuasive' effect, and will EU courts endorse their approach?

The long-term success of the GDPR also depends on its perceived effectiveness in imposing reasonable restraints on EU governments, not only on businesses. A significant threat to the GDPR comes from COVID-19 and State surveillance. The EDPB has stated that data protection rules, including both the GDPR and the ePrivacy Directive, do not hinder measures to fight a pandemic. They point to various legitimate grounds for processing, and exceptions, but stress that restrictions must be 'proportionate and limited to the emergency period'. COVID-19 is a daunting test of these requirements for GDPR credibility as a global standard.