

# About Finding Practical Solutions (Without the GDPR)

*Nico van Eijk\**

Every year the crème de la crème of privacy meets in September/October for the International Conference of Data Protection and Privacy Commissioners, the ICDPPC. This year the 39th conference was organised in Hong Kong by the local Privacy Commissioner for Personal Data. It was 18 years ago since the conference took place in Asia. I'm not a regular participant, but attended because researchers of my institute presented a very interesting study called 'A Roadmap to Enhancing User Control via Privacy Dashboards' (Authors are Kristina Irion, Svetlana Yakovleva, Joris van Hoboken and Marcelo Thompson).<sup>1</sup> The study was commissioned by the Privacy Bridges project. This project, bringing together EU and US experts, was set up a few years ago under the stewardship of Jacob Kohnstamm, the then chairman of the Dutch Data Protection Authority (DPA) and chairman of the Article 29 Working Party, to bridge differences in privacy between Europe and the US.<sup>2</sup> In order to become a bridge, three criteria need to be met. Bridges must involve practical steps that can be taken by defined actors within a reasonable time period. Bridges must not involve changes to constitutional principles or to the law and finally, bridges must have a positive effect on the level of privacy protection on both sides of the Atlantic. After finishing its report with defining ten possible bridges, the Privacy Bridges group decided to continue its work and to commission the aforementioned study with the objective to further investigate the second bridge. This bridge is about user control and calls on technology companies, privacy regulators, industry organisations, privacy scholars, civil society groups and technical standards bodies to come together to develop easy-to-use mechanisms for expressing individual decisions regarding user choice and consent. The outcome should be usable technology, developed in an open standards-setting process, combined with clear regulatory guidance from regulators, resulting in enhanced user control over how data about them is collected and used.

In light of the location of the conference, the researchers were asked to present solutions that would not only bridge Europe and the US, but could also work across other regions, including Asia. Based on a thorough selection process, the report focuses on privacy dashboards. These dashboards are well known and have a long history, but in recent times substantial improvements have been made and dashboards therefore have new potential. Or as the report states:

---

DOI: 10.21552/edpl/2017/3/5

\* Nico van Eijk is professor in Information Law at the Institute for Information Law (IViR, University of Amsterdam). He is also co-author of one of the articles in this issue.

1 See, Kristina Irion et al, 'A Roadmap to Enhancing User Control via Privacy Dashboards' (University of Amsterdam, 2017) <<https://www.ivir.nl/publicaties/download/PrivacyBridgesUserControls2017.pdf>> accessed 6 October 2017.

2 See, IViR and MIT, 'Privacy Bridges: EU and US Privacy Experts in Search of Transatlantic Privacy Solutions' (2015) <<https://privacybridges.mit.edu/>> accessed 6 October 2017.

Well-designed privacy dashboards currently represent, in our view, the most feasible strategy among those existing mechanisms and promising new approaches for enhancing user controls we reviewed. Privacy dashboards are user interfaces that provide as a single point of access to information on the collection and use of personal data as well as the configuration of privacy settings by users. At the present moment privacy dashboards represent a realistic scenario that is attuned to the online, mobile and platform economy and has gained traction in the market.

By focusing on user control, the study bypasses issues such as consent being the only way forward, and allows solutions for regions where giving explicit consent isn't at the core of privacy regulation or has a less prominent role.

This brings me back to the ICDPPC as such. Although its slogan was 'Connecting West with East by Protecting and Respecting Data Privacy' most of the discussions were mainly about promoting Western solutions, and not so much about building real bridges. To be truly honest, there was only one buzzword during the conference: GDPR, GDPR, GDPR. If for every time this abbreviation was mentioned one Euro or US Dollar had been collected for a charity, this charity would by now have had several millions deposited in its bank account! It almost looked like the privacy world has come to a standstill and is solely focused on 25 May 2018 when the GDPR becomes effective.

We have to move beyond this type of determinism. The world is not revolving around the GDPR. It seems the GDPR rhetoric is suffering from the famous Mark Twain quote, 'To a man with a hammer, everything looks like a nail.' We cannot call every problem in society a privacy or data protection issue nor should we attempt to: recently a privacy lawyer tried to convince me that contract law is a subset of privacy law because a contract contains personal data as the names of those signing are in it ...

If we look more carefully at the issues that cause so much turmoil in the privacy community, we must conclude that many of them are not about privacy as such. It's about companies not behaving the way companies should behave and who by doing so are disturbing the creation of a level playing field, and are damaging those who are entirely or largely compliant. Such problems should first of all be handled via competition law or other legal instruments concerning corporations. Consumers are being misled and their money is 'stolen' or ordered goods are not being delivered by the webstore. Such problems should first of all be handled via consumer law and regulation on unfair and deceptive business practices. To draw a parallel with another fundamental right: when I don't find the newspaper on my doormat, I don't call the newspaper claiming my fundamental right to receive information has been infringed. No, I call them and politely ask why they didn't deliver the goddamned paper!

If we continue to expand its reach, privacy and data protection becomes a black hole that sucks in everything. This would severely damage privacy as a fundamental right and turn it into a non-descript commodity. As every fundamental right advocate knows,

fundamental rights are so important that you can't attach a value to it and it should only be referred to as a last resort.

The GDPR is mainly about exploitation and monetisation, with the famous 4%-of-global-turnover fine as its crown jewel. Many GDPR-ists behave like ambulance chasers and use it for scaring clients. Of course, such a fine is highly unlikely. The measure comes from competition law where the maximum fine can even be 10% of global turnover. A competition lawyer can tell you what the real parameters are for this type of fines and how complicated the burden of proof is. He will also tell you that competition law has various remedies aimed at changing behaviour (such as binding agreements), remedies the GDPR is lacking.

It makes no sense to ignore the existence and reality of the GDPR and we will have to live with it. Nevertheless, we should prepare for and work on the post-GDPR era. This would require a tilting-process: Those elements in the GDPR that aren't primarily about privacy as a fundamental right, but are subsets of competition, consumer, or other more generic regulatory frameworks should first of all be dealt with via these frameworks, ie tilting from a vertical to a horizontal approach. Interestingly, the GDPR doesn't exclude such a tilting and basically recognizes a system of concurring competences. The article in this issue on unfair commercial practices further illustrates this.

It will be interesting to observe whether other regulators will pick up this challenge and step in. The Hong Kong conference showed the tremendous struggle of many DPAs to become a serious regulator. In particular, European DPAs or their observers expressed concerns about DPAs capabilities to enforce the GDPR due to a lack of enforcement-experience, budget and qualified personnel. Therefore, other regulators, including market, consumer and telecommunications regulators, might see a need or opportunity to take up their responsibilities from a more generic perspective. This could be done in close cooperation with the DPAs. By reversing the order and focusing first on a solution from a non-GDPR perspective has another great benefit: The generic approach will help to bridge differences between regions and jurisdictions as most of them have similar instruments put into place.

Next year's ICDPPC conference will be in Brussels hosted by the European Data Protection Supervisor (EDPS) and the Bulgarian DPA (Bulgaria will be the chair of the European Union when the conference takes place). The focus of the conference includes digital ethics. An excellent theme not just (or just not) to discuss the GDPR, but also to focus on alternatives.