Technological Forecasting & Social Change 116 (2017) 142–150

Contents lists available at ScienceDirect

Technological Forecasting & Social Change

The technology foresight activities of European Union data protection authorities

David Barnard-Wills

Trilateral Research, 72 Hammersmith Road, London, W14 8TH, United Kingdom

ARTICLE INFO

Article history:
Received 17 February 2016
Received in revised form 2 August 2016
Accepted 18 August 2016
Available online 14 November 2016

Keywords:
Data protection
Participatory foresight
Expert bodies
Privacy
Regulation

ABSTRACT

Data Protection Authorities play multiple roles, including education, consultancy, provision of policy advice, international coordination, as well as enforcement of regulation. In exercising these roles DPA's engage in a range of activities centred around understanding new technology developments, and anticipating their potential effects and impacts upon data protection and privacy. As responsible parties in relation to enforcement of national and EU data protection law DPAs are in a clear position to assess or provide guidance upon the requirements of the existing legal framework in relation to new technologies. This paper maps the technology foresight activities of European DPAs, the importance of this activity to their work, the particular challenges they face, and the extent to which such activities are performed in isolation or collaboration. It also assesses the potential for a collaborative EU DPA technology foresight task force.

1. Introduction

Data Protection Authorities (DPAs) are independent authorities (with their own powers and responsibilities, and that are organisationally separate from government[1]) with a supervisory role in relation to data protection. Globally, DPAs (also known as privacy commissioners, data privacy agencies and privacy enforcement authorities[2]) play multiple roles, including education, consultancy, provision of policy advice, international coordination, as well as enforcement of regulation.[3] Within the EU, they primarily draw their authority from the national implementations of the Data Protection Directive 95/46/EC. The data protection legal regime in the EU is currently undergoing a significant reform process: The General Data Protection Regulation (GDPR),[4] and the associated Police and Criminal Justice Data Protection Directive, are intended to reform and update the 1995 EU Data Protection Directive and replace the 2008 Framework decision.[5] This will further expand the roles of EU DPAs whilst at the same time increasing the harmonisation of their powers and increasing the level of cooperation between them.

Technology foresight encompasses a range of activities centred around understanding new technology developments, and anticipating their potential effects and impacts. In the context of DPA's roles and their collaborative activity (where this activity is sometimes also termed "technology watch") this focuses upon the potential impacts of emerging technologies upon data protection and privacy. Whilst there are many accounts of foresight approaches in information technology in general,[6] and privacy and data protection in particular,[7] as well as the technology foresight activities of national governments,[8] the foresight activity of data protection authorities has not been the subject of systematic study.

One reason for this is that technology foresight is not, for the most part an explicitly mandated task for EU DPAs. Further, many EU DPAs mandate as supervisory and enforcement agencies is a primarily reactive function. However, technology foresight prepares data protection authorities for enforcement action they may have to take in the future, but also allows them to intervene as stakeholders in the development of new technologies, and in particular better influence their adoption and deployment. Technology foresight activities allow regulators to get ahead of potential data protection problems and concerns. As responsible parties in relation to enforcement of national data protection law DPAs are in a clear position to assess or provide guidance upon the requirements of the existing legal framework in relation to new technologies. In this manner, technology foresight supports approaches such as privacy-by-design,[9] allowing for earlier intervention and for the better adoption and promotion of privacy-enhancing technology. It will also support DPAs in their role in data protection impact

E-mail address: david.barnard-wills@trilateralresearch.com.

[1] Thatcher (2002).
[2] OECD (2007).
[3] Bennett and Raab (2003, pp. 109-114).
[4] (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119/1).
[5] de Hert et al. (2013), Kuner (2012), Costa and Poullet (2012).
[6] Miles (2010).
[7] See for example, Wright et al. (2007) and Donohue and Ypsilanti (2009).
[8] See for example, Martin and Johnston (1999), Grupp and Linstone (1999).
[9] Ontario Information and Privacy Commissioner (2011).

http://dx.doi.org/10.1016/j.techfore.2016.08.032
0040-1625/

assessments under Article 35 of the GDPR, prior consultation under Article 36, and most significantly, the Article 57(i) obligation to "monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices".

It also allows regulators to better understand the fit between the existing regulatory framework, their enforcement and education strategies, and new technologies. Policy functions for technology foresight in data protection can include informing policy, facilitating policy implementation (including enforcement), embedding participation in policy making, supporting policy definition, through to guiding the full-scale reconfiguration of the policy system.[10] Technology foresight includes informal and formal methods (e.g. delphi surveys, expert panels, literature reviews and public consultations) but also importantly must include the way that products of technology foresight activity are communicated and shared. Technology foresight is therefore an information sharing issue as the activity produces new types of knowledge, the distribution of which is a key part of the activities' effectiveness. Therefore considering technology foresight activities by DPAs should also include the institutional arrangements, including collaboration, that surround it.

The PHAEDRA II project recently conducted a series of semi-structured interviews with senior representatives of European Data protection authorities between April and May 2015. The project interviewed 27 representatives, covering nearly all EU Member State national DPAs, one German state DPA (Landesbeauftragter für Datenschutz) representative[11] and the European Data Protection Assistant Supervisor.[12] Amongst other topics, the representatives of the EU DPAs were asked if their authorities conducted analyses of emerging technologies for potential privacy and data protection issues. We also asked if the results of any such activity were shared with other DPAs. We followed up by asking for their opinions and perspectives upon the value of a technology foresight "taskforce" to collectively engage in this activity. Many DPAs, particular smaller authorities, reported lacking the resources to conduct such activity in a systematic way, or to dedicate particular members of staff to this task. This did not mean that they did not have an interest in developing technologies, but that this interest was often pursued on an ad hoc basis by staff with other roles. Some DPAs reported that their learning about new technologies was driven by the complaints they received, the cases that they investigated, and external queries (e.g. from journalists). These smaller DPAs were interested in the technology watch activities of their larger peers, who have technology specialists, and saw value in learning from these. This present article builds upon these interviews, using short case studies of currently emerging technologies to examine the requirements for technology foresight in this field, identifies current technology foresight best practices, both at national levels and in collaboration including how this information is shared amongst EU DPAs, and explores the potential for a technology foresight "task force". The finding of the paper is that Technology foresight is an area where there is a high level of variation between DPAs in terms of both resources and experience. Some DPAs have developed sophisticated strategies for technology foresight, whilst others, often those with limited experience and resources, have been forced into an ad-hoc mode of technology foresight driven by complaints from the public. Foresight must be contextualised against the diversity of EU DPAs, with staff numbers ranging from 14 (Cyprus) to 350 (the UK).[13] Because the products of technology foresight can be shared between DPAs, there are substantial benefits to integrating technology foresight activity by DPAs, for example from resource-pooling, or the expansion of the technology sub-group of the Article 29 Data Protection Working Party's (the collective body of EU DPAs). This collaboration can be achieved relatively easily and under the DPAs' existing legal authority, but will require resourcing.

2. Emerging technologies and their privacy and data protection impacts

Technological foresight for data protection and privacy is complicated by four factors, as can be illustrated with examples from emerging technologies attracting data protection and privacy concerns, in this case drones, big data and Internet of Things (IOT).[14] Drones[15] are a varied and emerging technology with clear impacts for privacy and also for data protection, in particular in their use for law enforcement purposes, but also in civilian applications. Whilst many data handling and analysis practices might be called "big data", the actual concept of big data refers to data processing to do things at large scale, than cannot be done at a smaller one, and the extraction of new insights or the creation of new forms of value from massive data sets.[16] IOT and its various related technologies (such as smart cities, cars, homes etc.) involve the proliferation of sensors and actuators throughout the environment, and the interconnection of these devices with each other and with the online environment.[17] [18]

The first factor complicating DPA foresight is that understanding what new technologies are doing, and the real limits of their capabilities is hard, likely requiring domain expertise, and new approaches, whilst negotiating any marketing claims which may overstate technological capacities, whilst downplaying potential data protection impacts. The Article 29 Data Protection Working Party's Opinion on drones highlights the issue of data ownership, the requirement for clear identification of controller and processor, and advocates the use of data protection impact assessments in the deployment and use of drones[19] (as has the European Data Protection Supervisor).[20] Similarly, protecting privacy in big data may require greater accountability from big data processors, whilst institutions and professionals will need to develop the skills to assess and interpret the complex algorithmic decision making that will emerge.[21] The EDPS report on *Meeting the Challenges of Big Data* noted that business models exploiting new capabilities for massive collection, instantaneous transmission, combination and re-use of personal information for new purposes strain data protection principles, and highlighted the role of new principles such as accountability and privacy by design in responding to this challenge. It also noted the need for the EU to show leadership in developing accountable personal data processing, rather than uncritically importing data business models that have been developed elsewhere. The EDPS called for responsible and sustainable development of big data: organisations being transparent about the data they process, granting users a high degree of control over how their data is used, designing user friendly data protection into products and services, and being more accountable for what they do.[22]

Second, technologies do have particular "affordances" - relational properties which support particular types of actions[23] - but can also

[10] Da Costa et al. (2008).
[11] Given Germany's particular federal model of data protection authorities.
[12] Barnard-Wills and Wright (2015).
[13] Wright, David & Wadhwa, Kush, "Cooperation and coordination viewed by supervisory authorities themselves: results of the PHAEDRA surveys" in Paul De Hert, Dariusz Kloza & Pawel Makowski (eds), Enforcing Privacy: Lessons from current implementations and perspectives for the future, Wydawnictwo Sejmowe, Warsaw, 2015, pp.33–5.
[14] These selected technologies are sufficiently mature and have been the focus of enough attention to provide relevant material and identify details of the associated foresight practices, they are also actively debated on privacy and data protection grounds.
[15] Also known as unmanned aerial vehicles (UAV) or Remotely Piloted Aircraft Systems (RPAS).
[16] For the (multiple and contested) origins of the term, see Weinberg et al. (2013).
[17] IEEE (2015).
[18] Barnard-Wills et al. (2014).
[19] Article 29 Data Protection Working Party, Opinion 01/2015 on Privacy and Data Protection Issues relating to the utilisation of drones, Brussels, 16 June 2015. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp231_en.pdf, p.10.
[20] European Data Protection Supervisor (2014).
[21] Mayer-Schönberger and Cukier (2013, pp. 191).
[22] European Data Protection Supervisor, Op.Cit., p.4.
[23] Gaver (1991).