Technological Forecasting & Social Change xxx (2016) xxx–xxx

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 xxxx

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).

Please cite this article as: Barnard-Wills, D., The technology foresight activities of European Union data protection authorities, Technol. Forecast. Soc. Change (2016), http://dx.doi.org/10.1016/j.techfore.2016.08.032

be used in ways unintended by the designers and developers. The mutable nature of data technologies means these affordances can shift rapidly. Several affordances of drones contribute towards their privacy impact: drones provide new platforms and angles for visual surveillance, perform tasks that manned systems cannot for safety or economic reasons,[24] avoid ground-level barriers and congestion, follow targets, combine with other surveillance infrastructures[25] and place larger areas under surveillance and for greater periods.[26] Furthermore, several features of drones bring their operation into conflict with EU data protection legislation, particularly for meeting transparency, accountability and consent obligations,[27] incidental collection of personal data, and around what data is being transmitted from the drone to the operator, and for what purposes this is being processed. This lack of visibility (a "double invisibility"[28]) also increases the possibility of panoptic or chilling effects.[29] An ACLU study highlighted discriminatory targeting, institutional abuse, and automated enforcement, identifying drones as part of a trend towards law enforcement without human decision makers.[30] An EDPS Opinion on drones in civil aviation underlines the importance of Privacy Enhancing Technologies to ensure efficacy against privacy breaches.[31,32] Likewise, big data raises privacy and data protection concerns, due to the increased processing of data, and the potential to reveal information from data that was not previously possible, and therefore not anticipated (either by data subjects or by regulators). One of the drives to "big data" is to unlock latent knowledge and value in existing data sets. However this creates a clear conflict with purpose limitation and transparency requirements in EU data protection law. It also drives organisations to collect and store more data on the assumption that they can later extract some commercial value.[33] The aim of many IOT systems is to increase efficiency and control, but they also raise potential privacy (and security) risks, depending upon the way the technologies are deployed. The increased number of sensors and activity logs provide a source of close, granular and intimate personal data on the activities and behaviour of inhabitants and visitors. The IOT is therefore a point of intense contact between networked information technology and physical space.[34]

Third, technological development is not linear, and disruptive breaks can occur which bring about qualitative changes in circumstances, making prediction from past technologies problematic. For example, compared with CCTV, drones can be equipped with various payloads, can process different types of information, are not fixed to a single place, can enter private spaces, and can be deployed rapidly. These capabilities distinctly change their privacy impact. Future technological advances are expected to increase the range and duration of drone operation, whilst reducing size and cost, thereby increasing stealth and surveillance capacities.[35] However, the study for the EC found that drones did not present *new* data protection issues (their payloads are not new) and that their operation could be regulated through either existing data protection legislation, or under the new framework of the GDPR.[36] A Council of Europe report on big data states that "the statistical practices involved in Big Data-type analyses introduce a new way of sub-contracting to automatic systems the task of ensuring that the categories (of merit, need, desirability) which govern the distribution of resources and opportunities in our society emanate from this digital reality itself rather than their being instituted politically or agreed upon contractually".[37]

Finally, each technology cannot be taken in isolation, but should be assessed alongside the range of other technologies with which it may become combined. For privacy and data protection, the combination of data from various sources can have very significant impacts. The European Group on Ethics in Science and New Technologies has warned that "While regulation of separate functions e.g. in telecommunications or the use of DNA in identifying an individual has been possible, the real challenge will be in regulating combined functions".[38] For example, privacy concerns relate not only to drones as an aircraft, but also to the payload or software with which the drone is fitted.[39] The Article 29 Working Party's Opinion reiterates this "the relevant point from a privacy and data protection standpoint is not the drone per se but the data processing equipment on board the drone and the subsequent processing of personal data that may take place".[40] and that the "potential impact of the privacy intrusion is compounded by the wide constellation of stakeholders and entities involved in their use".[41] Trends in IOT suggest that developers wish to pursue the "digital mesh" where more and more devices are interconnected; increased machine learning and "ambient user experience" where interaction with IOT devices and services becomes more seamless across devices, and also less formal and screen based.[42]

Across the DPAs interviewed by PHAEDRA there was a strong sense that following technological developments was a very important task.[43] From these challenges we can extract the following considerations for collaboration between EU DPAs on technology foresight activities. Technology foresight requires a combination of domain expertise. It requires understanding the technologies involved, including their real capabilities and limitations, and changes in state-of-the art, as well as the direction of travel of key trends, and potential use. It also requires understanding the existing policy and regulatory environment in which these technologies may be deployed. Whilst DPAs are likely the best source of expertise on the data protection environment, emerging technologies will be deployed in diverse sectors (as demonstrated by the example technologies) and understanding their full privacy and data protection impacts will require some engagement with regulators and policy makers in those sectors. Third, it requires tools and approaches for understanding the potential social impacts of emerging technologies, as the technologies impact upon privacy and data protection cannot be assessed in isolation, or directly "read-off" from the technological affordances alone. There is a need for DPAs to ensure they have access to these capabilities, although not every DPA necessarily needs these in-house if access can be assured across the collective network of EU DPAs and their stakeholders. The same information collection and processing technologies are likely to be deployed across the EU Member States, making a strong argument for collective technology foresight activity.

3. A diverse landscape of technology foresight practices

Several existing practices in technology foresight by EU DPAs can be identified. These include technology foresight at national levels, information sharing through networks and events, and joint technology foresight activity through collective bodies such as the Article 29 Data Protection Working Party, the Berlin Group and the Consultative committee on Convention 108.

Many DPAs, in particular smaller authorities, reported that they did not have the resources to conduct such activity in a systematic way, or

[24] European RPAS Steering Group (2013, pp. 5).
[25] Clarke (2014a).
[26] Clarke (2014b).
[27] Finn et al. (2014, pp. 14).
[28] Fossool (2008).
[29] Finn et al., Op cit, 07 November 2014.
[30] Stanley and Crump (2011, pp. 12).
[31] European Data Protection Supervisor, Op. cit., 26 November 2014.
[32] Pauner and Viquri, 2015
[33] Mayer-Schönberger & Cukier, Op. cit., 2013, p.153.
[34] Ibid, p.iv.
[35] Stanley & Crump, Op. cit., December 2011.
[36] Finn et al., Op cit., 07 November 2014.
[37] Rouvroy (2016).
[38] European Group on Ethics in Science and New Technologies (2014, pp. 33).
[39] Finn et al., Op cit, 07 November 2017, p.40.
[40] Article 29 Data Protection Working Party, Op. cit., 2015., p.7.
[41] Ibid, p.8.
[42] Levy (2015).
[43] Barnard-Wills and Wright, 2015, Op.cit., p.29.

Please cite this article as: Barnard-Wills, D., The technology foresight activities of European Union data protection authorities, Technol. Forecast. Soc. Change (2016), http://dx.doi.org/10.1016/j.techfore.2016.08.032

to dedicate particular staff to this task.[44] This did not mean that they had no interest in emerging technologies, but that investigation of such was often done on an ad hoc or case-by-case basis by staff with other roles. Some DPAs felt that their learning about new technologies was somewhat 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 foresight activities of their larger peers, who have technology specialists, and saw value in learning from these. Some DPAs also noted that their technology foresight activity was often not shared with other DPAs.

As an example of this diversity, a survey of DPAs conducted in 2014 found that at the time only three had written positions on the use of remotely piloted aerial systems (drones) and that a further three were drafting positions. The majority of DPAs described themselves as having a "good" understanding of the potential civil applications of RPAS. The survey did find varying positions on how DPAs perceived the privacy, data protection and ethical risks emerging from the civil use of drones. 34% of DPAs responding to the survey reported that they had been involved in consultative activity on the civil use, with half of these responding to requests for consultation from their respective national civil aviation authorities, and a further two responding to the European Commission.[45]

3.1. Technology foresight at the national level

Some DPAs have specific expertise in this area, and provided information on their technology foresight methodologies, including the way that they drew in information from external bodies. This is supported by analysis of their policy documents and foresight output. For some EU DPAs conducting technology foresight and foresight activity is an explicit duty arising from their foundational legislation. The following paragraphs provide examples of this type of activity at the national level.

3.1.1. Studies and reports

La Commission nationale de l'informatique et des libertés (CNIL - the French DPA) publishes Innovation and Prospective (IP) reports to present the findings of future studies carried out by CNIL's DEIP - Department for Future Studies, Innovation and Foresight and by its innovation lab, one of the largest such departments in the EU. The first three Newsletters on Innovation and Foresight were published in both French and English. Since 2013, they have continued in French roughly twice a year, and there have been two subsequent collections of IP reports published in French in May 2014[46] and October 2015.[47] These were collected together into the report *Privacy Towards 2020: Expert View* in 2013.[48] This report covered a very wide range of topics, including the social internet, algorithmic decision making, geolocation, biometrics, nanotechnology, digital identity and innovations in regulation. The methodology for the report was interviews conducted with 42 multi-disciplinary experts. In relation to collaboration and coordination, the introduction to the report also sets out a philosophy for technology foresight activity by the French DPA:

> "[CNIL] must develop its analysis in the area of forecasting to better understand technological developments and new uses, and to anticipate and assess the new key issues for data protection. It must be confirmed as a pragmatic and credible regulator that is capable of proposing operational solutions. It must therefore invest, as far at its means permit, in research conducted in these fields, and in piloting and commissioning work that it considers to be of particular importance.".[49]

This strategy includes establishing a Department for Foresight in 2011, the publication of the IP reports, but also building up a research community composed of researchers, developers, and sector experts on issues of data protection (both in France and internationally), in order to discover new solutions and support periodic self-examination. In the PHAEDRA II interviews, CNIL reported a close relationship and an intensive exchange of information between this Department and the Technology Subgroup of the Art. 29. Working Party.

Commission de la Protection de la vie Privée (CPVP - Belgium) publishes thematic dossiers on keys areas of data protection. Some focus on data protection in particular practices or sectors (e.g. credit, elections or direct marketing), other focus on particular technologies (e.g. cameras, biometrics, eID, and genetic information).[50]

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) in Germany has published information on several emerging technology issues in its annual progress reports, including use of drones, big data, the Internet of Things.[51] The Hellenic Data Protection Authority in Greece has done the same, recently covering topics including smart meters, biometric fingerprint recognition, and new technologies in web services.[52] The Spanish Agencia Española de Protección De Datos (AEPD) covered big data and the Internet of Things in its 2016 *Memoria AEPD*.[53] The Hungarian National Authority for Data Protection and Freedom of information (NAIH) addressed its general approach to technology foresight in its annual report for 2014, whilst focusing upon biometric technologies, the national identity card systems, and association codes (temporary sequences that facilitate establishing lawful links between different data processing activities). The report stated:

> "Researching the conditions of enforcement of information rights we can identify a complicated structure of aspects including legislation, legal awareness, social values and the acceptance of information rights. Although, beyond the effects of the above mentioned factors belonging mostly to the society, the consequences of the technical-IT development are becoming more remarkable."[54]

The Information Commissioner's Office (ICO - UK) website news section and blog frequently cover emerging technologies amongst other topics with data protection implications.[55] ICO has also produced initial guidance on drones.[56] The TietoSuoja ("Privacy Policy") magazine published by the Data Inspection Board, (Finland) in collaboration with the Data Protection Ombudsman, Finnish Communications Regulatory Authority, and the Patent and Registration Office, published general consumption articles that are related to technology foresight alongside other data protection and privacy related topics.[57]

3.1.2. External expert panels

Several DPAs, including CNIL,[58] maintain an external expert panel to support their technology foresight activities. The ICO uses what it describes as an "intelligence hub" model for technology foresight activity, intended to bring together intelligence and information coming into the Office from different sources, including journalists, academia, and technologists. The Dutch DPA reports that it "is actively following relevant technical and legal developments and remains in contact with different stakeholders, such as branch-, consumer- and human rights organisations".[59] Small DPAs often rely upon the personal knowledge and networks of their staff. Representatives from DPA are frequent attendees at relevant conferences and events,

[44] Barnard-Wills & Wright, Op. cit., 2015, p.29.
[45] Finn et al., Op. cit., p.155.
[46] CNIL (2014).
[47] CNIL (2015a).
[48] CNIL (2013).
[49] Ibid, p.05.
[50] CPVP, n.d.
[51] Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (2015).
[52] Hellenic Data Protection Authority (2014).
[53] Agencia Española de Protección De Datos (2015).
[54] National Authority for Data Protection and Freedom of Information (2015, pp. 18).
[55] ICO, n.d.-a.
[56] ICO, n.d.-b.
[57] Tietosuoja, n.d.
[58] CNIL, n.d.
[59] College Bescherming Persoonsgegevens, n.d., pp. 3.

Please cite this article as: Barnard-Wills, D., The technology foresight activities of European Union data protection authorities, Technol. Forecast. Soc. Change (2016), http://dx.doi.org/10.1016/j.techfore.2016.08.032

and these networks can be quite significantly developed. DPAs have also developed working relationships with industry groups, such those representing the smart meter industry.[60]

3.1.3. Working with academia and EU-funded research projects

Several EU DPAs maintain good relationships with external researchers, and have previously funded research projects into particular technological developments (and their social and legal consequences). For example CNIL's 'Mobilities' collaboration with INRIA on research into smart phone ecosystems. This project ran over three years and identified massive numbers of points of access to personal data from smart phone that are invisible to users.[61] It also highlighted that many smart phone apps were inaccessible "black boxes" to regulators as much as they are to users. This research project also allowed CNIL to conduct some primary research, in this case developing a method to monitor data access and communication behaviour of apps live in a real world context, trialled on smart phones carried and used by CNIL personnel. The study had particular insight into roles of smart phones as carriers of identity, the central importance of location data, and the role of the operating system for determining the rules of personal data collection by app designers. Luxembourg's CNPD engaged in a collaborative study into legal issues in data protection, cloud computing and privacy in collaboration with the University of Luxembourg.[62]

3.1.4. Learning from previous technologies

Learning from regulatory experiences with previous technologies whilst paying attention to salient differences is a relatively common strategy that is a part of technology foresight practices - for example, the Article 29 Data Protection Working Party opinion on drones draws upon guidance already developed for CCTV, in particular pointing out that whilst there is no specific legislation on the data protection implications of drones, there may be national provisions applicable to CCTV systems, that may also apply in the case of drones.[63] The Irish DPA's guidance on drones adopts the same stance.[64] Likewise the CNIL approach to the Internet of Things is based upon existing work on Smart Meters.[65] These approaches can save time, effort and costs, but they still require understanding the key differences between new technologies or practices and their antecedents, which again requires a level of technical knowledge and access. For example, ICO revised its code of practice on CCTV in 2014 precisely because of the emergence of new technologies (from ANPR to drones).[66] Ireland did similar with their CCTV guidance in December 2015, updated at the same times as they released new guidance on body-worn cameras and drones.[67]

3.2. DPA collaboration on technology foresight

In addition to technology foresight activities conducted at the national level, which could be adapted and adopted to the EU (or even international level) we can identify current practices in international collaborative technology foresight between EU DPAs.

Information on technology trends and potential future risks is exchanged by DPAs through working parties, joint events, and the personal networks of technology specialists. Many DPAs highlight the existence of the **Article 29 Data Protection Working Party's Technology Sub-Group** as an area where this activity is already taking place (including recently on the Internet of Things, wearable devices and cloud computing[68]). The sub-group allows for information sharing, but also for concerns to be raised, and for collaborative activity to be discussed and agreed upon (recently, this has included informing counterparts about investigations into Google, Microsoft, LinkedIn and Facebook).[69] The Technology sub-group works upon the working papers that become Article 29 Opinions.[70] Recently, these have included Opinions on anonymisation techniques and device fingerprinting, and active involvement in the Opinion on the Internet of Things.

The transition to the EDPB might recompose this group. However some DPAs suggested that the activity of the Technology Sub-Group was primarily driven by responding to issues raised by the plenary meeting of the Working Party, for example, supporting the production of Opinions, and that this did not leave much capacity for horizon scanning (in much the same way as individual DPAs). Some technology foresight activity, particularly that of the Art. 29 Working Party is conducted in response to calls from the European Commission and other actors for opinion or guidance. For example the Article 29 Data Protection Working Party's Opinion on drones arises from a request from the European Commission for practical advice for legislators and regulators (at both the European and national level, including Civil Aviation Authorities (CAA), industry, policy officers, and the public at large).[71] The EDPS opinion on big data was explicitly drafted to be consistent with the approach taken by the Article 29 Data Protection Working Party on data protection aspects of new technologies.[72]

Additionally, the **International Working Group on Data Protection in Telecommunication** ("Berlin Group")[73] was identified by various DPAs as another grouping of DPAs already engaged in some technology-foresight activities and a good forum for information exchange. Over recent years, the Berlin group has produced working papers on emerging technology topics including privacy principles under pressure in the age of big data analytics, privacy and aerial surveillance, wearable computing, web tracking, smart meters, online payments, and vehicle tracking.[74] These are conventionally published in both German and English. The Berlin Group working paper on big data was used as the basis for the Resolution adopted by the International Conference of Data Protection and Privacy Commissioners (ICDPPC) in Mauritius in October 2014.[75]

In addition to formal networks and groupings, smaller networks can be brought together for specific tasks. For example, following on from its Opinion on big data, the EDPS organised stakeholder consultation workshops with policy makers, one of their key constituencies, to draw attention to the data protection and privacy challenges associated with this new technology.[76] Publications of research reports are often supplemented by public events allowing for additional stakeholder input. DPAs have also collaborated in activities in this domain conducted by third parties (for example, workshops, expert panels, surveys, etc). When multiple DPAs participate this can be considered a form of externally-driven collaborative technology foresight. An example of this is the involvement of several DPAs in the consultation process leading to the Cloud Security Alliance (CSA)'s development of Privacy Level Agreements for the sale of cloud computing services in the EU in 2013.[77]

[60] Taieb and Gérot (2015).
[61] CNIL (2015b).
[62] University of Leuven (2011).
[63] Article 29 Data Protection Working Party, Op. cit., 16 June 2015, p.8.
[64] Data Protection Commissioner, Ireland (2015).
[65] Taieb & Gerot, Op. cit.
[66] Bamford (2014)
[67] Data Protection Commissioner Ireland, n.d.
[68] Article 29 Data Protection Working Party (2013).
[69] National Authority for Data Protection and Freedom of Information, March 2015, Op. cit. p.72. http://www.naih.hu/files/Annual-report_NAIH_2014_EN_FINAL_v4.pdf.
[70] Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Op. Cit., 2015, http://www.bfdi.bund.de/SharedDocs/Publikationen/Taetigkeitsberichte/TB_BfDI/25TB_13_14.pdf;jsessionid=79B2677CD70DD83882F957B77C86C5E2.1_cid319?__blob=publicationFile&v=10.
[71] Article 29 Data Protection Working Party, Op. cit., 16 June 2015.
[72] European Data Protection Supervisor, Op. Cit, 19 November 2015, https://www.huntonprivacyblog.com/files/2015/11/15-11-19_Big_Data_EN.pdf.
[73] Berliner Beautragter für Datenschutz und Informationsfreiheit, n.d.
[74] The working papers and common positions adopted by the Working Group are available at: http://www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt/working-papers-and-common-positions-adopted-by-the-working-group.
[75] Commission de la protection de la vie privee (2014, pp. 39).
[76] Hunton and Williams (2015).
[77] Privacy Level Agreement Working Group (2013).

Please cite this article as: Barnard-Wills, D., The technology foresight activities of European Union data protection authorities, Technol. Forecast. Soc. Change (2016), http://dx.doi.org/10.1016/j.techfore.2016.08.032

Alongside these EU collaborative activities, the **Council of Europe's Consultative Committee of Convention 108** has also produced reports on challenges to the rights to privacy and data protection from emerging technologies, including a report on nanotechnology, ubiquitous computing and the Internet of Things[78] as well as mapping trends in other areas of data protection,[79] including the automated inter-state exchange of personal data for tax and criminal justice purposes.[80] These reports are primarily developed for the committee by academic domain experts.

Sitting part way between individual and collaborative technology foresight, DPAs engaged in technology foresight activities are highly likely to monitor and draw upon publications and research by their peers, including those outside the EU. For example, the Berlin Group's working paper on wearable technologies acknowledges that it draws heavily upon work conducted by the Office of the Privacy Commissioner of Canada, as well as Opinions from the Article 29 Data Protection Working Party, press, and academic research papers.[81]

4. Moving beyond best practice

Based upon this existing practice, this paper now offers two proposals for areas in which best practices could be expanded, first by increasing the degree to which DPA foresight draws upon wider publics and networks, and second by increasing the degree of intra-DPA collaboration on foresight.

4.1. Moving beyond best practice I - participatory foresight

Technology foresight activities by EU DPA seem primarily based on expert-driven foresight models, where technology experts (internal or external to the DPA), academics and industry stakeholders are consulted to understand technological impacts. There are an increasing number of participatory foresight methodologies. This attempts to expand the categories and types of stakeholder involved in the assessment process, including public consultation, but also bringing in the major new users of technologies in the public sector (including law enforcement agencies). A feature of participatory foresight is that the process through which the assessment is conduct is seen as being as important as the final insight. The activity of wider consultation, includes more people, builds networks, and improves the way that any resulting policy is implemented (as it is likely to have greater support). There is not yet much evidence of DPAs deploying this form of participatory technology foresight, however there are suitable resources available. As well as ongoing work in the field of technology assessment (which has a greater purchase in some Member States than others), several recent European research projects have developed public consultation methodologies for privacy and security technologies, which might be deployed in future by DPAs.[82] Basing DPA technology foresight upon public participation does however face several limitations, including different cultural attitudes towards both privacy, and public deliberation, and the problems encountered when knowledge about technologies deliberated on is not widely shared.[83,84] The Constructive Technology Assessment focus on reflexivity and the participation of a wide range of actors, in order to "broaden technology development by including more aspects and more actors and at an early stage so as to hopefully realise better technology in a better society"[85] offers potential for DPAs. Whilst the focus upon short term design and construction is in tension with strategic approaches to foresight with a medium-term horizon, the value in "making the future" through increasing dialogue and understanding between deliberative participants and identifying opportunities for intervention in the innovation process[86] cannot be underestimated for DPAs. Shelly-Egan et al. have developed a set of good practice advice for design, delivery and evaluation of participatory methods that is applicable to the work of DPAs.[87]

Given the technological neutrality of EU data protection legislation (both in its previous form, and in the GDPR) it may not be necessary for data protection authorities to conduct any primary research into new technologies as part of their technology foresight, but rather position themselves as informed consumers of existing primary research into technology and advisors into structured research funding processes such as the EU's Horizon 2020 scheme. However, given constraints on the type of socially, legally, and ethically informed research into new technologies required to understand data protection impacts, data protection authorities, both individually and collectively, can serve as an important driver, commissioner and clearing house in this field. Collectively, the capacity to commission, conduct and disseminate such research is increased.

4.2. Moving beyond best practice II - technology foresight task force

The PHAEDRA II project explored the potential for a collective "Technology foresight task force" organised amongst DPAs at the EU level. Collecting together technology experts from European DPAs into a technology foresight taskforce, with the capability to better share expertise, seemed to have some support from DPAs.[88] For some DPAs the Article 29 Working party Technology Subgroup was seen as already acting as such a task force for the moment, however, others suggested that the need to respond to the Working Group's plenary, and relatively small scale, left less capacity for science and technology-driven foresight. As we have seen, this activity is currently unequally dispersed across individual DPAs.

A specific task force, set-up to include foresight activity on data protection and privacy issues, offers the following benefits:

- Established regular channels of communication would speed up the transfer of information. EU DPAs are faced with the same emerging technologies therefore there is much potential for collaboration in this area, and especially to reduce the repetition of work.
- A centralised, collaborative body for technology foresight would also be a clear source for information, and could act as a clearing house for insight developed at national levels.
- For industry and stakeholders, the body would be able to provide consistent guidance, applicable across the Member States.
- Collective technology foresight could also allow for increased professionalisation of technology foresight and assessment methods through shared learning.
- It would allow pooling of research budgets to support more in-depth technology assessment activity, which would then be distributed across all participants.

[78] Miller and Matthew (2013).
[79] Korff and Brown (2013).
[80] Porassor and Aouizerat (2014).
[81] International Working Group on Data Protection in Telecommunications, 2015.
[82] See for example, Van Lieshout and Barnard-Wills (2015); as well as www.securitydecisions.org/about-dessi; The ASSERT Toolkit for Society Impact Assessment in Security Research, http://assert.maisondx.com/; The SUPRISE project: http://surprise-project.eu/; and The PACT Project: http://www.projectpact.eu/.
[83] Biegelbauer, Peter and Loebner, Anne, "The challenge of citizen participation in democracy" Sociological Series, No.94, Institute of Advanced studies, Vienna, 2010.
[84] Schedler, Petra and Glastra, Folke "Communicating policy in late modern society: on the boundaries of interactive policy making", Policy and Politics, vol.29, No.3, 2001, pp. 337–349.
[85] Schot, Johan and Rip, Arie, "The Past and Future of Constructive Technology Assessment", Technological Forecasting and Social Change, No.54, pp.251–268, 1997.
[86] Rip, Arie and te Kulve, Haico "Constructive Technology Assessment and Socio-Technical Scenarios" in Erik Fisher, Cythia Selin, Jameson M. Wetmore (Eds), The Yearbook of Nanotechnology in Society, Volume 1: Presenting Futures, Berlin, Springer, 2008, pp. 49–70.
[87] Shelly-Egan, Claire, Wright, David, Bencin, Rok, Sumic Riha, Jelica, Strle, Gegor, Oviada, Daniela, Pastor Canedo, Adelina, Angeli, Christine, and Sotiriou, Menelaos, SATORI Deliverable D2.1: Report (Handbook) of participatory processes, July 2014, http://satoriproject.eu/media/D2.1_Report-handbook-of-participatory-processes_FINAL1.pdf.
[88] Barnard-Wills & Wright, Op. cit., 2015, p.29.

Please cite this article as: Barnard-Wills, D., The technology foresight activities of European Union data protection authorities, Technol. Forecast. Soc. Change (2016), http://dx.doi.org/10.1016/j.techfore.2016.08.032

- Similarly, the task force could pool stakeholder consultation activities and expert panels, with some limitations imposed by language differences and paying attention to local differences (e.g. the way an industry operates in one country as opposed to another).
- The task force might also be able to conduct or contribute to forensic IT investigations where smaller DPAs lack the capacity for this.
- A shared foresight programme may also serve as a mechanism to bring EU DPAs into closer cooperation, both through increased experience of collaborative working amongst the task force participants, but also promoting a shared and commonly accepted perspective on policy-relevant technological developments, as these participants inform and educate their colleagues using the knowledge gained in the task force.
- The greater weight of a collaborative technology foresight body may contribute towards the ability to argue for the different interests of society in technology development and deployment and achieving a balance between them and commercial concerns.

The GDPR strongly alters the nature of the Article 29 Data Protection Working Party, which will be recomposed into the European Data Protection Board (EDPB),[89] with unclear impacts for technology foresight and the Technology Sub Group, but a more substantial legal personhood, an important role in consistency between national DPAs, and more powers than the Article 29 Working Party.[90] Technology foresight activities were not explicitly included in the Article 29 Working Party's statement on the 2016 action plan for the implementation of the General Data Protection Regulation.[91] However, this change offers the potential to explicitly construct an appropriate and effective technology foresight taskforce, particularly based upon the roles of the board under Article 70 of the GDPR, the Board could (at least) continue the activities of the Technology Subgroup, supported by its secretariat. Technology foresight contributes towards the tasks of issuing guidelines, recommendations and best practice, examining the application of the regulation, and providing opinion and advice to the Commission. The board looks formally capable of hosting such a task force, but would require appropriate staff and resources. If the board possessed the institutional capacity to host a technology foresight task force, team or department, then this group should have a high level of interaction with similar roles located within national and regional EU DPAs (potentially including secondment and joint projects if possible). DPAs further suggested that in the future, representatives from additional DPAs could be integrated to the sub-group depending on their resources.

Participation in a technology foresight task force need not be limited to DPAs, although this has some risk of expanding the remit of the group to the extent that its focus is diluted. The EDPS has called for a *digital regulation clearing house*, where all authorities with a role in regulation in the digital world (including both data protection and competition regulators) can coordinate their activity,[92] and a technology foresight task force could contribute to such an effort. Whilst one DPA linked technology foresight to encouraging technology companies to perform more Privacy Impact Assessments (PIAs), another DPA issued a caution that a technology foresight task force should be staffed by DPA personnel in order to ensure that it was not overly influenced by major technology companies. As a consequence, an independent site of technological expertise was seen as important. The formal independence of its participants would be a key element of the legitimacy of a task force, and this means ensuring the role of DPAs, and limiting the role of external participants.

There are potentially problematic elements of a collective foresight body. Certain technological developments attract uneven public attention across EU Member States. DPAs may feel under greater pressure to investigate technologies that have attracted public controversy in their own countries (for example Google Street View). This may require that some capacity is retained for DPAs to act individually with regard to technology foresight. However, if the focus of technology foresight activity is technologies that are further away from deployment, then few authorities will be able anticipate if these technologies are likely to present a local issue or not. A related issue is that DPAs may play a role translating existing work on the privacy implications of new technologies into Member State languages. For example the Estonia DPA remarked in its 2014 annual report that "Drafting guidelines is particularly important considering the smallness of the Estonian language and legal space. With the help of indicative and explanatory guidelines, we attempt to make up for the shortage of judicial practice regarding the right to privacy, IT laws, and the scarcity of specialised literature (press)."[93] Centralised technology foresight should not be set up in such a way that prevents this diffusion of knowledge regarding the data protection issues of emerging technologies. Whilst DPA foresight is significantly distinct from innovation support foresight, such a task force would have to identify its role in relation to the existing networks of national and parliamentary technology assessment bodies, and bodies at the European level such as the European Parliament's Science and Technology Options Assessment (STOA), and the European Parliamentary Technology Assessment (EPTA) network, so as to maximise synergies and avoid duplication. Such bodies advise parliaments on the possible social, economic and environmental impact of new sciences and technologies, and do encompass changes in social relationships from ICT, which would lead to some thematic overlaps with DPAs. Understanding the potential and challenges of the internet, science policy, communication and global networks are both priority areas for STOA.[94] Not all member states have such bodies[95] and the emerging European PTA landscape is marked by heterogeneity and diversity.[96] This activity is mostly focused upon the needs of national parliaments,[97] making cross-EU activity challenging, in particular in finding a European policy audience, but there are EU-level initiatives, conferences and projects.[98] This highlights the importance of learning from parallel mechanisms as well as tying the activities of a DPA task force closely to the tasks and roles of DPAS under the GDPR.

Establishing a Technology Foresight Task Force would have the following additional requirements:

- The capacity to contribute personnel and/or budgets and the scope of such a task force would still have to be negotiated and agreed. There is a potential collective action problem in that the products of the task force are likely to be shared broadly, even beyond direct participants.
- When interviewed, several DPAs reiterated the importance that any technology foresight task force should be composed in a manner that ensures that it retains its independence, particularly from large technology companies. This could include being staffed primarily by data protection authority personnel, and drawing primarily upon independent experts for additional information and insight.
- The Task Force should be composed of a combination of IT specialists and experts from other fields (including law, social sciences), and ideally with experience across the scope of DPA operations.

[89] Section 3, Articles 68 to 76 of Regulation (EU) 2016/679.
[90] De Hert, Paul & Papakonstantinou, Vagelis, "The new General Data Protection Regulation: Still a sound systems for the protection of individuals?", Computer Law & Security Review, in press, 2016.
[91] Article 29 Data Protection Working Party, Statement on the 2016 action plan for the implementation of the General Data Protection Regulation (GDPR), Brussels, 2 February 2016.
[92] Butarelli (2015).
[93] Peep (2015).
[94] European Parliament Science and Technology Options Assessment, "About", available online: http://www.europarl.europa.eu/stoa/cms/home/panel/projects.
[95] Boavida and Moniz (2015).
[96] Holm et al. (2015).
[97] Borland, M., Bütschi, D., Leichteris, E., and Peissl, W., "Doing cross-European Technology Assessment" in L. Klüver, R. Nielsen and M Jørgensen (Eds.) Policy-Oriented Technology Assessment Across Europe: Expanding Capabilites, Palgrave Macmillan, 2016, p.78.
[98] Ganzevelas and Van Est (2012).

Please cite this article as: Barnard-Wills, D., The technology foresight activities of European Union data protection authorities, Technol. Forecast. Soc. Change (2016), http://dx.doi.org/10.1016/j.techfore.2016.08.032

- NESTA, a UK innovation organisation, recommends (in general) that foresight activities are perhaps best located within other strategic and policy development activities, rather than in isolated programmes.[99] Therefore there should remain strong ongoing communication between the task force, the EDPB and the different DPAs.
- The appropriate pooling of consultation activities should be determined by the intended policy activity and its relation to the EU data protection regime. For example, if technology foresight is intended to facilitate policy implementation, which will be related to a specific context, then the activity should be more focused upon that context. The more abstract the level of the technology foresight activity (when the activity is focused upon understanding new technologies absent a particular site of deployment) then this can be more easily generalised between Member States, and therefore more easily shared between DPAs. If the aim of the technology foresight activity is to generate interaction between regulators and regulated, then this should be conducted at more local levels.
- Finally, the mandate and "horizons" of the task force should be collectively agreed by contributing parties to ensure that the task force is sufficiently resourced to be able to not only engage with existing technologies and their challenges but also (and perhaps more importantly) with "foreseeing", assessing and dealing with emerging technologies and technology trends.

5. Conclusions

Technology foresight activities are important for EU DPAs and the importance of this type of activity is only likely to increase given the potential volume and complexity of impacts upon privacy and data protection from emerging technologies, and the tasks under the GDPR. Whilst many DPAs are engaged in technology foresight activities, either through specific foresight programmes, maintaining links to sites of expertise, developing internal expertise, and through the informal accumulation of technology knowledge through reactive and responsive investigations, not all DPAs are able to conduct this activity. Collaborative technology foresight amongst DPAs is a relatively under-developed area which would benefit strongly from further joint working, in addition to increasingly professionalising technology foresight in privacy and data protection and developing sector-specific techniques and approaches. Technology foresight and technology foresight information sharing is an area that would strongly benefit from intra-DPA cooperation which would not be legally or technically difficult, but would require some resource commitments. The creation of a formal technology foresight task force (or its evolution from the Article 29 Data Protection Working Party technology sub-group) offers several significant benefits for responding to future technology developments with potential impacts upon privacy and data protection. Additionally, the technology foresight context is a strong setting for bringing together interested parties (DPAs, industry and civil society interest groups) to discuss potential issues early so as to avoid problems in the future. The links that can be built, and the common goals that can be established in participatory foresight can be useful also in other areas of DPA activity, including education, guidance and the provision of policy advice.

Acknowledgements

This article is based upon research conducted as part of the PHAEDRA II project ("Improving practical and helpful cooperation between data protection authorities" and the article is possible due to the assistance and contribution of all project partners. The project is co-funded by the European Union and the Fundamental Rights and Citizenship Programme (JUST/2013/FRAC/AG6068), however the contents of this article are the sole responsibility of the authors and cannot be taken to represent the views of the European Commission. More information on the project can be found at http://www.phaedra-project.eu/. Thanks to Antonella Galetta, Cristina Pauner, Dan Svantsson and Sophie Kwasny for reviewing earlier drafts of parts of the paper.

[99] Cassingena Harper (2013).

References

Agencia Española de Protección De Datos, 2015. Memoria AEPD 2014, Madrid. http://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/common/memorias/2014/Memoria_AEPD_2014.pdf.

Article 29 Data Protection Working Party, 2013. Work programme 2014-2015, 3 December 2013, Brussels. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp210_en.pdf.

Bamford, J., 2014. New Technologies Mean New CCTV Code. Information Commissioner's Blog (20 May, https://iconewsblog.wordpress.com/2014/05/20/new-technologies-mean-new-cctv-code/).

Barnard-Wills, D., Wright, D., 2015. Authorities' views on the impact of the data protection framework reform on their co-operation in the EU, PHAEDRA II project deliverable 1. http://www.phaedra-project.eu/wp-content/uploads/PHAEDRA2_D1_20150720.pdf.

Barnard-Wills, D., Marino, L., Portesi, S., 2014. Threat Landscape and Good Practice Guide for Smart Homes and Converged Media. ENISA, Heraklion (1 December).

Bennett, C., Raab, C., 2003. The Governance of Privacy: Policy Instruments in Global Perspective. MIT Press, Cambridge MA & London.

Berliner Beautragter für Datenschutz und Informationsfreiheit, i. International working Group of Data Protection in telecommunications (IWGDPT)http://www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt accessed 24 December 2015.

Boavida, N., Moniz, A., 2015. Technology Assessment in Non-PTA Countries: An Overview of Recent Developments in Europe. FCT:IET Working Paper Series (December).

Butarelli, G., 2015. Competition Rebooted: Enforcement and Personal Data in Digital Markets. Keynote Speech at Joint ERA-EDPS Seminar, Brussels (24 September, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2015/15-09-24_ERA_GB_EN.pdf).

Cassingena Harper, J., 2013. Impact of Technology Foresight. Nesta Working Paper, no 13/16 (November, https://www.nesta.org.uk/sites/default/files/1316_impact_of_technology_foresight_final_version.pdf).

Clarke, R., 2014a. Understanding the drone epidemic. Comput. Law Secur. Rev. 30, 230–246.

Clarke, R., 2014b. What drones inherit from their ancestors. Comput. Law Secur. Rev. 30, 247–262.

CNIL, 2013. Privacy towards 2020: Expert Views. IP Reports, No.01 (http://www.cnil.fr/fileadmin/documents/en/CAHIER_IP_EN2.pdf).

CNIL, 2014. Le Corps, Nouvel Objet connecté: Du Quantified Self à La M-Santé: Les Nouveaux Territoires de La Mise en données Du Monde. Cahiers IP No.2 (May, http://www.cnil.fr/fileadmin/documents/La_CNIL/publications/DEIP/CNIL_CAHIERS_IP2_WEB.pdf).

CNIL, 2015a. Les données, Muses et frontières de La création - Lire, écouter, Regarder et Jouer à l'heure de La Personnalisation. Cahiers IP, No.3 (October, http://www.cnil.fr/fileadmin/documents/La_CNIL/publications/DEIP/CNIL_CAHIERS_IP3.pdf).

CNIL, 2015b. Mobilitics, Season 2: Smartphones and their Apps under the Microscope. CNIL News (27 January, http://www.cnil.fr/english/news-and-events/news/article/mobilitics-season-2-smartphones-and-their-apps-under-the-microscope/).

CNIL, d. Le Comité de la prospectivehttp://www.cnil.fr/linstitution/ip/comite-de-la-prospective/ accessed 24 December 2015.

College Bescherming Persoonsgegevens, d. Annual report 2014 (English summary)https://www.cbpweb.nl/sites/default/files/atoms/files/annual_report_2014.pdf.

Commission de la protection de la vie privee, 2014. Rapport annuel 2014, Brussels. https://www.privacycommission.be/sites/privacycommission/files/documents/Rapport%20annuel%202014.pdf.

Costa, L., Poullet, Y., 2012. Privacy and the regulation of 2012. Comput. Law Secur. Rev. 28, 254–262.

CPVP, d. Aperçu de nos dossiers thématiqueshttps://www.privacycommission.be/fr/dossiers-thematiques (accessed 24 December 2015).

Da Costa, O., Warnke, P., Cagnin, C., Scapolo, F., 2008. The impact of foresight on policy-making: insights from the FORLEARN mutual learning process. Tech. Anal. Strat. Manag. 20 (3), 369–387.

Data Protection Commissioner, Ireland, 2015. Guidance on the use of drones. 22 December. https://www.dataprotection.ie/docs/Guidance-on-the-use-of-Drone-Aircraft/1510.htm.

Data Protection Commissioner Ireland, d. Data protection and CCTVhttps://www.dataprotection.ie/viewdoc.asp?m=m&fn=/documents/guidance/cctv.htm (accessed 11 January 2015).

de Hert, P., Papakonstantinou, V., Wright, D., Gutwirth, S., 2013. The proposed regulation and the construction of a principles-driven system for individual data protection. Innovation 26 (1–2), 133–144.

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, 2015i. Tätigkeitsbericht zum datenschutz für die Jahre 2013 und 2014, Bonn. http://www.bfdi.bund.de/SharedDocs/Publikationen/Taetigkeitsberichte/TB_BfDI/25TB_13_14.pdf;jsessionid=79B2677CD70DD83882F957B77C86C5E2.1_cid319?__blob=publicationFile&v=10.

Donohue, M., Ypsilanti, 2009. Cloud Computing and Public Policy. ICCP Technology Foresight Forum. OECD (14 October, http://www.oecd.org/internet/ieconomy/43933771.pdf).

European Data Protection Supervisor, 2014. Opinion on the Communication from the Commission to the European Parliament and the Council on "a New Era for Aviation - Opening the Aviation Market to the Civil Use of remotely Piloted Aircraft Systems in a Safe and Sustainable Manner", Brussels (26 November).
European Data Protection Supervisor, 2015. Opinion 7/2015 meeting the challenges of big data: a call for transparency, user control, data protection by design and accountability, Brussels. 19 November. https://www.huntonprivacyblog.com/files/2015/11/15-11-19_Big_Data_EN.pdf.
European Group on Ethics in Science and New Technologies, 2014. Opinion on Ethics of Security and Surveillance Technologies, No. 28, Brussels (20 May).
European RPAS Steering Group, 2013. Roadmap for the Integration of Civil remotely Piloted Aircraft Systems to the European Aviation System (June).
Finn, R.L., Wright, D., Donavan, A., Jacques, L., De Hert, P., 2014. Privacy, Data Protection and Ethical Risks in Civil RPAS Operations, D3.3 Final Report for the European Commission (07 November).
Fossool, V., 2008. RFID et biométrie - état Delieuex. In: Pullemans, D.B.A. (Ed.), Actualities Du Droit de La Vie privée. Bruylat, Brussels, pp. 149–150.
Ganzevelas, J., Van Est, R., 2012. TA Practices in Europe. Deliverable 2.2 in the Collaborative Project on the Mobilization and Mutual Learning Actions in European Parliamentary Technology Assessment (PACITA).
Gaver, W.M., 1991. Technology Affordances. ACM (http://www.it.hiof.no/interaction-design/papers/gaver1991ta.pdf).
Grupp, H., Linstone, H.A., 1999. National technology foresight activities around the globe: ressurection and new paradigms. Technol. Forecast. Soc. Chang. 60 (1), 85–94.
Hellenic Data Protection Authority, 2014. Annual report. http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/ANNUALREPORTS/AR2015/ANNUAL%202014%20V2.0%20WEB%20VIEW.PDF.
Holm, J., Merz, C., Scherz, C., 2015. Identity shaping: challenges of advising parliaments and society: a brief history of parliamentary technology assessment. Philos. Sci. Technol. 20 (2), 164–178.
Hunton, Williams, 2015. EDPS Issues Opinion on the Challenges of Big Data. Lexicology (25 November, http://www.lexology.com/library/detail.aspx?g=141e46da-24f6-4dfc-b1b7-1d2a464dafd9&utm_content=buffer90749&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer, accessed 24 November 2015).
ICO, d. Current topicshttps://ico.org.uk/about-the-ico/news-and-events/current-topics/ (accessed 24 december 2015).
ICO, d. Droneshttps://ico.org.uk/for-the-public/drones/ (accessed 24 December 2015).
IEEE, 2015. Towards a Definition of the Internet of Things (IoT). Issue 1, IEEE Internet Initiative (13 May, http://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Issue1_14MAY15.pdf).
International Working Group on Data Protection in Telecommunications, 2015. Working Paper on Privacy and Wearable Computing Devices, 27–28th April, Seoul.
Korff, D., Brown, I., 2013. The Use of the Internet & Related Services, Private Life & Data Protection: Trends & Technologies, Threats and Implications (T-PD(2013)07Rev, 31 March).
Kuner, C., 2012. The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law. Privacy and Security Law Report. The Bureau of National Affairs (02/06/).
Levy, H., 2015. Top 10 Technology Trends Signal the Digital Mesh. Gartner (7 October, https://www.gartner.com/smarterwithgartner/top-ten-technology-trends-signal-the-digital-mesh/).
Martin, B.R., Johnston, R., 1999. Technology foresight for wiring up the National Innovation System: experiences in Britain, Australia and New Zealand. Technol. Forecast. Soc. Chang. 60 (1), 37–51.
Mayer-Schönberger, Cukier, K., 2013. Big Data: A Revolution that will Transform how We Live, Work and Think. John Murrary, London.
Miles, I., 2010. The development of technology foresight: a review. Technol. Forecast. Soc. Chang. (77).
Miller, G., Matthew, K., 2013. Nanotechnology, ubiquitous computing and the internet of things: challenges to the rights to privacy and data protection: draft report to the Council of Europe, T-PD(2013)08, Strasbourg. 20 September. https://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD%282013%2908%20-%20Report%20Miller%20Kearnes%20-%20Nano%20privacy%20Draft%20report%20%28final%29.pdf.
National Authority for Data Protection and Freedom of Information, 2015r. Annual report 2014, Budapest. March. http://www.naih.hu/files/Annual-report_NAIH_2014_EN_FINAL_v4.pdf.
OECD, 2007. Recommendation on cross-border co-operation in the enforcement of laws protecting privacy, Paris. http://www.oecd.org/internet/interneteconomy/38770483.pdf.
Ontario Information & Privacy Commissioner, 2011. Privacy by design: strong privacy protection - now and well into the future, Ontario. https://www.ipc.on.ca/images/Resources/PbDReport.pdf.
Pauner, C., Viguri, J., 2015. A legal approach to civilian use of drones. Privacy and personal data protection concerns. Democr. Secur. Rev. 5 (3) (http://www.democraziaesicurezza.it/Saggi/A-Legal-Approach-to-Civilian-Use-of-Drones-in-Europe.-Privacy-and-Personal-Data-Protection-Concerns).
Peep, V., 2015. Summary by the Director-General. Annual Report: Summary. Estonian Data Protection Institute (http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/aastaettekanne%202014%2C%20ingl.pdf).
Porassor, C., Aouizerat, B., 2014. Report on the Implications for Data Protection of the Growing Use of Mechanismsm for Automatic Inter-State Exchanges of Personal Data for Administrative and Tax Purposes, as well as in Connnection with Money Laundering, Financing of Terrorism and Corruption. Bureau of the Consultative Committee of the Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data, Strasbourg (30 January, https://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD-BUR%282014%2901%20-%20Rapport%20CE%202013%20%28final%29%20C.%20Porasso_En.pdf).
Privacy Level Agreement Working Group, 2013. Privacy level agreement outline for the sale of cloud Services in the European Union, cloud security alliance. February. https://downloads.cloudsecurityalliance.org/initiatives/pla/Privacy_Level_Agreement_Outline.pdf.
Rouvroy, A., 2016. "of data and men" fundamental rights and freedoms in a world of big data, Council of Europe, Bureau of the Consultative Committee of the convention for the protection of individuals with regard to automatic processing of personal data [ETS108], Strasbourg. 11 January. http://www.coe.int/t/dghl/standardsetting/DataProtection/TPD_documents/T-PD-BUR%282015%2909REV_Big%20Data%20report_A%20%20Rouvroy_Final_EN.pdf.
Stanley, J., Crump, C., 2011. Protecting Privacy from Aerial Surveillance: Recommendations for Government Use of Drone Aircraft. ACLU, New York (December).
Taieb, S., Gérot, M., 2015. CNIL Head of Compliances Explains Approach on Connected Devices, Including Smart Meters. Chronicle of Data Protection. Hogan Lovells (22 October, http://www.hldataprotection.com/2015/10/articles/international-eu-privacy/cnil-head-of-compliance-explains-approach-on-connected-devices-including-smart-meters/).
Thatcher, M., 2002. Regulation after delegation: independent regulatory agencies in Europe. J. Eur. Publ. Policy 9 (6).
Tietosuoja, d. https://www.tietosuoja-lehti.fi (accessed 24 December 2015).
University of Leuven, 2011. How to Handle Data Protection in a Globalised World: The CNPD and the SNT Conclude a Partnership Agreement. Press Release, Luxembourg (17 November, http://wwwen.uni.lu/press/press_releases/2011/how_to_handle_data_protection_in_a_globalised_world_the_cnpd_and_the_snt_conclude_a_partnership_agreement_17_november_2011).
Van Lieshout, M., Barnard-Wills, D., 2015. Deliverable 11.3: The PRISMS Decision Support System. PRISMS Project (17 July, http://prismsproject.eu/wp-content/uploads/2015/07/PRISMS-d11-31.pdf).
Weinberg, B.D., Davis, L., Berger, P.D., 2013. Perspectives on big data. J. Mark. Anal. 1 (4), 187–201.
Wright, D., Gutwirth, S., Friedewald, M., 2007. Shining light on the dark side of ambient intelligence. Foresight 9 (2), 46–59.

Dr. David Barnard-Wills David is a Senior Research Analyst at Trilateral Research, a UK research company focusing on public policy and strategy in areas of new technologies. He has conducted research for Trilateral on privacy and security certification schemes, public attitudes to privacy and security, data protection policy and governance, cyber security of smart homes and societal impact assessment. His current work involves supporting cooperation between data protection authorities as part of the PHAEDRA II project. He has a PhD in Political science from the University of Nottingham on the politics of surveillance in the United Kingdom and has previously been a Research Fellow at Cranfield University, The University of Birmingham and The UK's Parliamentary Office of Science and Technology.

Please cite this article as: Barnard-Wills, D., The technology foresight activities of European Union data protection authorities, Technol. Forecast. Soc. Change (2016), http://dx.doi.org/10.1016/j.techfore.2016.08.032