Data protection authorities and information technology

Data Protection Authorities and Information Technology

Charles Raab*· & Ivan Szekely*

**University of Edinburgh, Scotland*
*** Eotvos Karoly Policy Institute, Budapest*

ABSTRACT

The ability of data protection authorities (DPAs) to gain and deploy sufficient knowledge of new technological developments in their regulation of personal-information practices is an important consideration now and for the future. However, DPAs' capacity to keep abreast of these developments has been questionable, and improvements in this are a matter of concern, especially given DPAs' task requirements under the European Union's (EU) General Data Protection Regulation (GDPR). This article reports the findings of a recent survey of EU DPAs that explore the problems they have in comprehending new technologies and how they are dealing with them.

Keywords: data protection authorities, supervisory authorities, privacy, information technology, General Data Protection Regulation, survey, technological competence

1. Introduction

In the field of information privacy, the overwhelming focus of scholarship for several decades has been on the legal and – increasingly – the technological dimensions of data protection; far less attention has been devoted to understanding the work of regulatory organisations, of which data protection authorities (DPAs) are the most prominent. Nevertheless, the efficacy of legal regimes for protecting personal data relies heavily on the way DPAs perform their tasks, and arguably more than on the letter of the law as seen in statutes and in the connoisseurship of legal scholars. Countries are frequently criticised for only passing laws to protect privacy without also creating implementation machinery that gives the law force through the institutional machinery by means of which compliance, good practice, and other requisites can be encouraged or required; the US is the most prominent case-in-point. Privacy law 'on the ground' rather than 'on the books', in the terms used by Bamberger and Mulligan (2015) in their study of corporate privacy behaviour, involves not only the work of chief privacy officers (CPOs) but of DPAs, with whom those non-state actors frequently engage in relationships that may only be structured vaguely by what the laws say 'on the books'. DPAs play a major role in arbitrating the degree of information privacy that we enjoy as a fundamental right. Their institutional arrangements, provenance, independence, and performance

· Corresponding author: Professor Charles Raab, Politics and International Relations, School of Social and Political Science, University of Edinburgh, Chrystal Macmillan Building, 15a George Square, Edinburgh EH8 9LD, Scotland, UK
Email address: c.d.raab@ed.ac.uk

are crucial to that enjoyment, but are less frequently, less systematically, and less comparatively investigated than many of the other components of data protection regimes.

DPAs are multi-taskers. Describing them as 'supervisory authorities', as is done in the European Union's (EU) General Data Protection Regulation (GDPR) (2016), or as 'regulatory authorities', only hints vaguely at one element of the range of activities that they are legally required to do and – less formally – that they are expected to do in the eyes of politicians, the public, and the mass media. Flaherty's (1997: 175) inventory of DPAs' includes 'oversight, auditing, monitoring, evaluation, expert knowledge, mediation, dispute resolution, and the balancing of competing interests'. With greater simplification, Jóri (2015) draws attention to two functions: 'shaping' (privacy advocacy) and 'applying' (mediating or enforcing). Referencing decisions of the European Court of Justice, Schütz (2012) highlights the independence of DPAs and its importance for regulatory functions. Bieker (2017) also mentions this, but focuses upon some forthcoming changes wrought by the GDPR and describes enforcement, complaints-handling, and co-operation across DPAs. The wide-ranging and deep discussion of DPAs by Hijmans (2016: 347-412) considers them as 'expert bodies', but only mentions in passing the relationship between technical knowledge and that expertise. He also points out the way in which the multiple roles of DPAs may involve them in conflicts and compromise their core, compliance-related task, although it is that multiplicity that has made them strong actors in the protection of information privacy.

The survey conducted by the Estonian DPA about the detailed competence and activities of European DPAs distinguishes the following categories: General competence (in the area of personal data protection and in freedom of information matters); educational and consultative activities (answering questions, adoption of guidance texts, approval of self-regulatory acts, training sessions and other public events, media work, including social media); supervision and enforcement activities (mediation, comparative survey, notice without investigation, preventive audit, registration, authorisations regarding data transfer to 3rd countries, prior checking, investigation and resolving of infringements, resolutions); policy advising, and additional activities.[1] Article 57(1) of the GDPR lists twenty-two 'tasks' that Member States' supervisory authorities are required to carry out, ending with the omnibus task 57(1)(v), 'fulfil any other tasks related to the protection of personal data'. This extraordinary range demands activity to be conducted under some twenty-six specified powers (investigative, corrective, authorization and advisory) conferred under Article 58. Under the GDPR, there are new role requirements or role expectations, a new impetus towards co-operation and institutionalised or informal interaction, but layered on top of the older inventory of roles. The complete 'package' will no doubt require new skills, new resources, and new uncertainties as DPAs face a future in which the possibility of regulation, and thus of protecting people's data and rights, is challenged by new patterns of data processing and new uses for personal data.

Bennett and Raab's (2006: 133-143) pastiche categorisation of what DPAs do outlines seven major tasks, or roles, in which these authorities are engaged as they implement law and oversee practice: ombudsman, auditor, consultant, educator, policy adviser, negotiator, and enforcer. This disaggregation of the institution of a DPA was not intended to be a definitive and universally found catalogue of activities performed by DPAs, much less to imply that all DPAs' performances were necessarily similar. However, it served as an analytical instrument for investigating what DPAs do and how they do it. Some DPAs might emphasise enforcement; others might concentrate on

[1] http://www.aki.ee/en/inspectorate/typology-dpa-s

educating the public ('data subjects') and companies or other organisations ('data controllers'). Some are more closely involved than others with advising on policy and legislation, or with negotiating such instruments as codes of practice. Thus the styles and strategies of DPAs in their regulatory roles are not uniform across the landscape of European or global data protection.

What is uniform, however, is their need to understand the data protection and information privacy implications of globally used information and communication technologies (ICTs), large-scale analysis of personal data by a variety of interests, and emerging technologies such as emotion-detection and predictive data analytics. Nearly thirty years ago, before the dawn of the modern Internet and, since then, the further dramatic advances in ICTs and their exploitation by states and private companies, Flaherty noted that DPAs 'monitor and evaluate new technological developments in data processing and telecommunications. Each agency has specialists in various types of information systems and data flows who can speak intelligently about data protection and security with the operators of government information systems' (Flaherty, 1989: 383). In 1983, Simitis (1983: 177) similarly wrote that these authorities 'have the necessary knowledge enabling them to analyze the structure of public and private agencies and to trace step by step their information procedures. They can therefore detect deficiencies and propose adequate remedies'.[2] Perhaps that was true of the relatively few DPAs at that time in the larger countries of the EU,[3] but is it still the case today, when the technological explosion, the proliferating demands placed upon DPAs, and the growth in their numbers across the EU at national and sub-national levels cast some doubt on their ability to deploy such knowledge in their activities 'on the ground'?

Based on the EU-funded PHAEDRA II project, Barnard-Wills (2017) examines this issue in the context of exploring the possibility of an institutionalised 'technology watch' or foresight capability across EU DPAs, building upon existing but fragmented activity, and referring both to the new co-operation requirements mandated by the GDPR. Semi-structured interviews with DPAs conducted in PHAEDRA II, as well as documentary analysis, showed the variable extent of ICT-related understanding and activity amongst DPAs and elicited explanations for these levels. The separate investigation reported in the present article aims to provide further and somewhat complementary statistical information on the current picture and on the reasons underlying the patterns revealed by DPAs' answers to a questionnaire-based survey of their attitudes and practices.

2. The survey and its methodology

This article attempts to cast light on this subject by reporting the findings of an empirical survey of all EU DPAs that was conducted in late 2015 and early 2016. The survey was organised to coincide with a public panel discussion on DPAs' understanding of ICT that was chaired and moderated by the authors in the Computers, Privacy and Data Protection (CPDP) conference[4] held in Brussels in January 2016.[5] The discussion was structured along the questions of the survey, and the

[2] Quoted in Flaherty (1998): 383, note 33.
[3] Research conducted in the 1990s by one of the authors suggests that the UK's Office of the Data Protection Registrar, the precursor of the Information Commissioner's Office that operated under the 1984 Data Protection Act and was headed by a computer scientist, nevertheless had only a limited and intermittent in-house capability to keep abreast of ICT development and use in the organisations it regulated.
[4] CPDP is one of the most important annual international multi-stakeholder professional events in the intersection of the areas indicated in its name, with around thousand participants from academia, business and government, see http://www.cpdpconferences.org
[5] The four panelists were: Amandine Jambert (CNIL, France), Achim Klabunde (EDPS), Marit Hansen (ULD-Schleswig-Holstein), and John Borking (formerly Registratiekamer, The Netherlands). We are grateful

participants – all of whom had significant expertise in this topic – were faced with the results of the survey analysis: their on-site evaluation and comments added important aspects to the findings of the survey.

This survey aimed to find out the extent to which DPAs were abreast of changes in ICTs with which personal data are processed and which powerfully shape the terrain on which DPAs' regulatory and supervisory activities take place. The authors' interest in this subject was fuelled by a perception that DPAs – among other shortcomings – were particularly deficient in their understanding of ICTs, so that their ability to regulate information processing would be compromised by deficiencies in their comprehension of technological changes that had important consequences for the protection of rights to privacy and data protection. It has become commonplace to assert that 'technology outpaces law' and that regulation therefore lags behind, and may indeed be futile if it does not adapt to changing technology-led circumstances. Moreover, it is not just that 'technology' might be far in the lead, but that both the data controllers who use it (and their consultants) and the privacy and human-rights activists who seek stronger regulation often possess much greater ICT expertise and knowledge than is demonstrated by the 'official' regulators. In this article, we are not obliged to align ourselves with this definition of the situation and to the pessimistic conclusions to which many commentators are led. However, the survey casts light on the current situation in the EU, on the brink of the inauguration of the GDPR in 2018, and as major consequent changes to the position of DPAs are about to take place.

We aimed to gather information from all EU Member State DPAs, plus the sub-national DPAs of several EU countries as well as the European Data Protection Supervisor (EDPS). Considering the heavy workload of these authorities, we compiled a short but carefully designed questionnaire that was e-mailed to relevant officials in the supervisory authorities.[6] It was not our aim to evaluate the expertise of DPAs in information and communication technologies, nor to test their knowledge in this field. This would have certainly resulted in contestable results and exceeded our capacity and mandate. Instead, we attempted to learn the DPA respondents' self-reported opinion on the expertise and capacity of their DPAs, and on the expertise of the community of DPAs in general. We also wanted to know whether the DPAs deem their expertise adequate for their present activities and for the challenges of the foreseeable future. The survey included questions on the proportion of the organisations' investigations involving technological aspects or requiring specific ICT expertise, as well as on the DPAs' preferences regarding proactive or reactive strategies in influencing privacy-related ICT matters.

In accordance with the explicit request of certain contacted authorities, we guaranteed the anonymity of the respondent organisations: even when individual responses were publicly presented, we do not reveal the identity of the organisation. In addition, where the organisational data, e.g. the number of employees, would have made it possible to identify certain DPAs, we applied the method of topcoding, that is, data values above an upper bound were truncated to threshold.

---

for their participation in the panel, and for their agreement to allow us to use some of the remarks they made in the CPDP panel session. The video recording of the panel discussion is available at https://www.youtube.com/watch?v=nwiXB0w5Mss

[6] The questionnaire is reproduced in Annex A.

The survey covered the Member States and sub-jurisdictions of the European Union and the European Economic Area, as well as Switzerland and the European Data Protection Supervisor (EDPS). The contacted organisations included 32 national and 46 sub-national[7] DPAs. In all, 79 agencies were contacted in late September 2015, with a deadline for completing the questionnaire by 30 November. Most contacted organisations - after several reminders - sent their responses in November, a few others by the end of the year. Before the public discussion of the survey findings at the CPDP conference in January 2016, we received responses from 44 DPAs (55.7% response rate), including 25 national authorities (78.1% response rate) and 19 sub-national DPAs (41.3% response rate). Three organizations joined the survey after the public discussion of the results, their responses have been included in the updated statistics presented in this paper.

This number of responses proved to be sufficient to allow meaningful analysis of the findings without unwarranted claims being made for their representativeness of the totality of DPAs. The size and diversity[8] of the sample did not encourage us to apply sophisticated statistical analyses; however the combination of descriptive data – along with textual explanations and the comments of the panel participants – revealed important characteristics of the DPAs' approach to, and expertise in, new information technologies. Statistics of this sort would require follow-up research using other techniques, such as interviews and inspection of documents, but these were beyond the scope of this survey exercise. Many respondents took advantage of the opportunity to write explanatory comments in the free-text part of the questionnaire, and the CPDP panel's experts gave further observations about the general issues being explored, without necessarily commenting on the situation regarding the DPAs in which they worked. The audience of the public discussion – including several DPAs' members – also had the opportunity to vote on certain questions posed by the moderator, and to voice their consent, dissent, comments and suggestions regarding the survey findings and the discussion. In the following we also take these contributions into consideration when analysing the survey findings and drawing conclusions. Thus the findings provide a basis for discussion, diagnosis and policy-related observations in the light of the overall legal requirements as well as social and organisational expectations of the roles that DPAs play at present and in the foreseeable future.

2.1. DPAs' expertise in information technologies

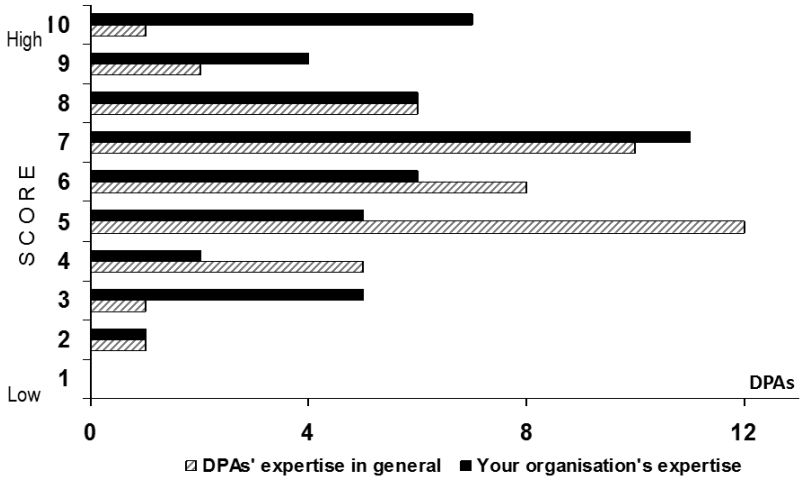
The survey included a question about how the data protection authorities evaluate the expertise of DPAs in general in the area of information and communication technologies. Most respondents[9] ranked the expertise of DPAs in general at medium level (between 5 and 7 on a numerical scale of 10 degrees), no authority evaluated the DPAs' level of expertise at the lowest level, and only one respondent evaluated it at the highest level. However, when asking the respondents to evaluate the level of expertise in ICT in their own organisation, the figures were somewhat higher: DPAs tended to evaluate their own expertise higher than that of the community of DPAs (Fig. 1).

[7] For example, the data protection authorities of the federal states of Germany, or those of the cantons of Switzerland.

[8] The biggest organisation had 379 employees, while the smallest one had a staff of a single person.

[9] In 22 cases (50% of the contacted organisations) it was the Commissioner him/herself, someone on behalf of the DPA, or a responsible leader of the organisation who responded; in 9 cases it was a communications officer or someone responsible for international affairs who returned the questionnaire; in 2 cases an IT professional filled it in, and in 11 cases the position of the person belonged to another category or was unknown.

Fig. 1. DPAs' expertise in information and communication technologies

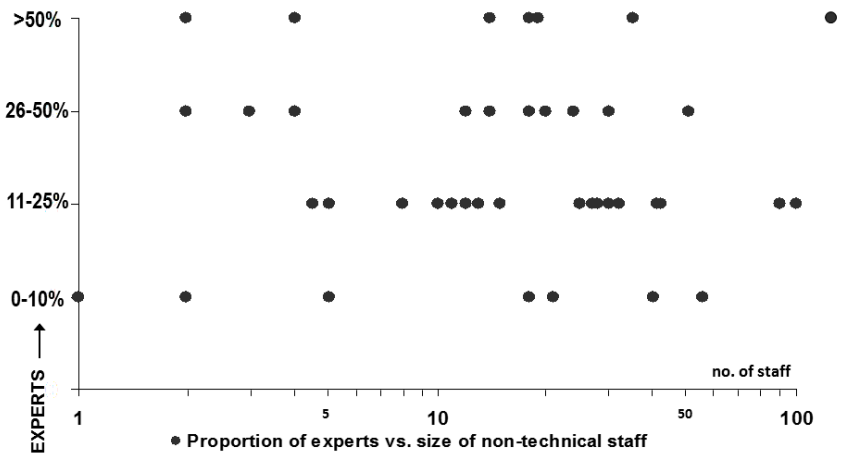


In the opinion of two of the panellists, this was due to a psychological characteristics of the institutions: they see themselves in a better position than that of 'the others'.[10]

The following questions required factual answers: we wanted to know the number of people on the staff of the DPAs in regulatory, policy, legal, investigatory or management positions, and the self-reported proportion of these staff members who have expertise in, or significant familiarity with, ICT. In Fig. 2 the size of non-technical staff is measured from 1 to 100 on the logarithmic X axis, the four categories offered for indicating the proportion of experts are listed on the Y axis. The analysis showed that the size of non-technical staff do not correlate with technical expertise: low proportion of expertise (0-10%) can be found at small and large DPAs alike, similarly to the highest level of expertise (>50%).

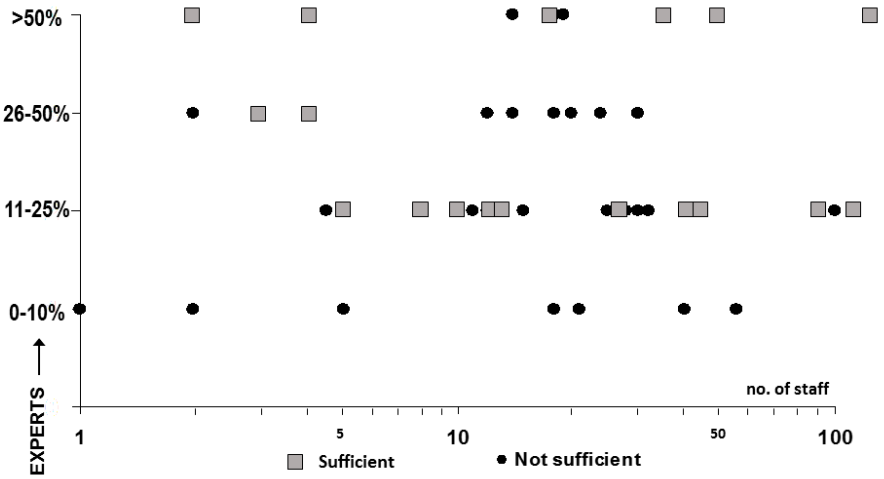
[10] This is a well-known phenomenon in empirical surveys when individuals' opinions are asked; perhaps this is also true in the case of organisations. The overwhelming majority of the audience of the public discussion, when voting on a question asked by the moderator, were of the opinion that the technical expertise of European DPAs in general was not 'adequate for the challenges of today and the foreseeable future'.

Fig. 2. ICT expertise of non-technical staff at DPAs



We also wanted to learn whether the respondent DPAs were satisfied with the indicated proportion of expertise for their work. None was satisfied with the lowest proportion (0-10%) of expertise, but in the three other categories no clear correlation between the level of satisfaction and the proportion of self-reported expertise could be established. In Fig. 3, in a setting similar to that of Fig. 2, the square (green) dots indicate those DPAs that regarded the proportion of expertise among their non-technical staff satisfactory, the round (red) dots indicate those who regarded this proportion unsatisfactory. In the 11-25% category about the same number of organisations evaluated this proportion as satisfactory and unsatisfactory, evenly distributed on the scale of the DPAs' size. Even in the highest category (>50%) there were some DPAs that regarded this level of expertise in ICT unsatisfactory.

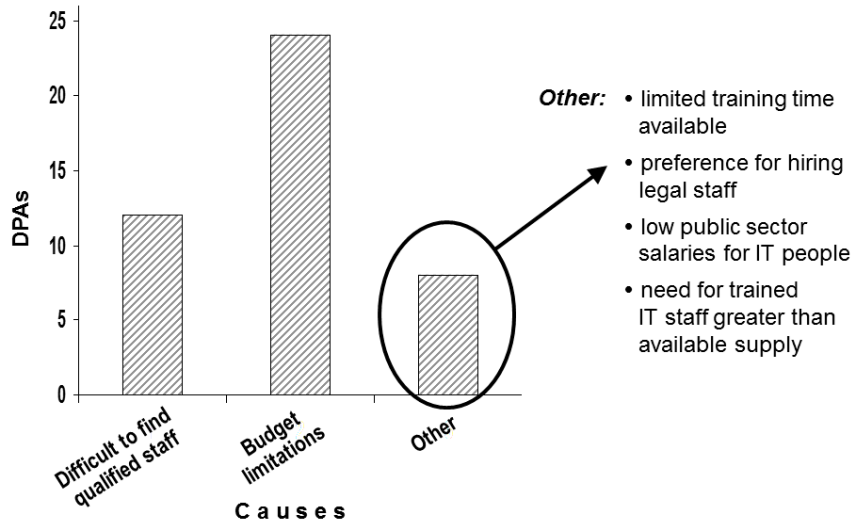
Fig. 3. Level of ICT expertise of non-technical staff at DPAs



Those who were not satisfied with the existing level of ICT expertise among the members of their non-technical staff were asked about the causes of the shortfall. The most popular answer was

budget limitations, followed by the difficulties in finding qualified staff. The remaining answers included the limited training time available in ICT-related matters, and the DPAs' preference for hiring legal staff over hiring ICT experts; the fact that salaries for ICT experts in the public sector are significantly lower than in the private sector, making such positions at DPAs less attractive; and finally, that the need for trained IT staff is far greater than the available supply (Fig. 4).[11]

Fig. 4. Not sufficient expertise: Causes of the shortfall



2.2. The necessary ICT expertise in investigations

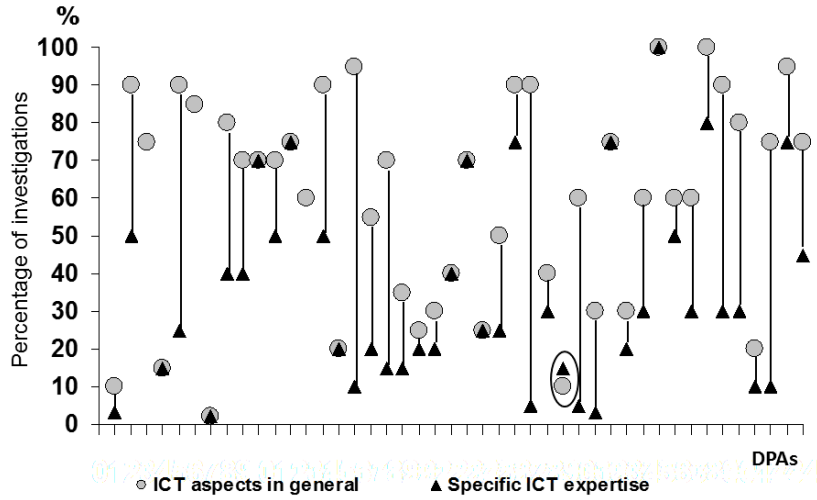
The survey included a question about the percentage of the respondent organisation's investigations (responding to data subjects' complaints or initiated by the DPA itself) that involve *general* ICT-related aspects (such as the use of computerised databases or the Internet). In the next question we asked the respondents about the percentage of investigations that require *specific* ICT expertise.

If we visualise the responses to the two questions on a joint scatter diagram, it can be seen that the majority of the respondents clearly distinguished the two categories and reported two significantly different percentages, although the general significance of ICT in their investigations shows big differences. In Fig. 5 the respondent organisations are represented on the X axis, while the percentages of the investigations are indicated on the Y axis; the round (green) dots represent the reported percentage of investigations involving ICT-related aspects in general, the triangle (red) dots represent the percentage of investigations requiring specific ICT expertise. The vertical lines connecting the round and the triangle dots show the distance between the two, that is, the difference between the two types of investigations belonging to the same DPA. A few DPAs reported the same percentage in the two categories – interestingly, in the lowest and highest range alike.[12]

[11] The PHAEDRA II inquiry (Barnard-Wills 2017: 143) found that resource limitations were an important reason given by some DPAs, especially smaller ones, for their inability to undertake much 'technology foresight' activity except when this is driven by complaints.

[12] The only DPA that reported a higher percentage of investigations requiring specific expertise than those involving ICT-related aspects in general (see circled) must have misunderstood the question. At this point in the CPDP panel session, the moderator posed a somewhat provocative question to the audience: whether data controllers, in particular service providers, can mislead DPAs in ICT-related matters. From the three options:

Fig. 5. DPA investigations involving ICT aspects *in general* and those requiring *specific* ICT expertise



Both the analysis of the survey results and the opinions presented at the public discussion showed that the present level of expertise available in the DPAs' offices is either not satisfactory or at least needs to be further enhanced. With regard to rapid technological developments and their impact on the processing and use of personal data, it seems evident that even the mere preservation of the existing level of ICT expertise in an organisation requires continuous learning. Therefore it was important to learn whether DPAs prefer developing their own expertise in-house or importing it from external sources, and the reason for their preferences.

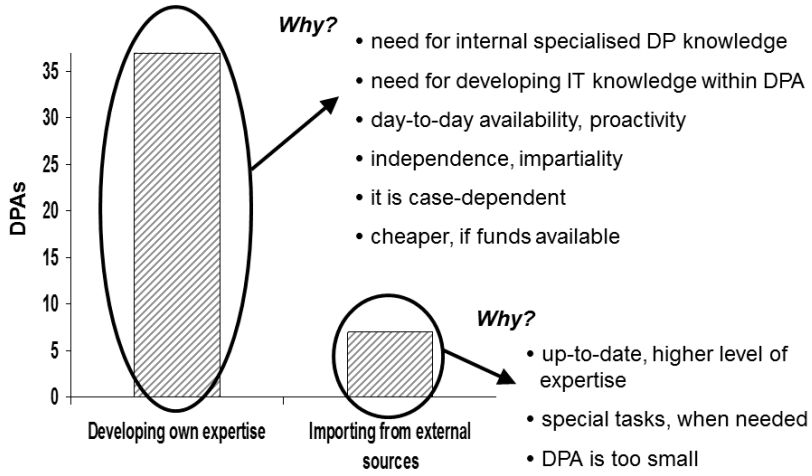
The survey found that the predominant opinion among DPAs was in favour of developing the necessary information technology expertise in the framework of their organisations and only a few DPAs thought that relying on the expertise of external ICT professionals was a better solution (Fig. 6). Among those that preferred in-house developing of expertise and explained their choice, the following reasons deserve noting:

- in the field of privacy and data protection, IT professionals need special knowledge, not only in legal terms but also in the technologies of processing personal data, and such a knowledge can be developed to the required level within DPAs and more easily in the course of practical audits of data controllers;
- ICT expertise has to be continuously available in-house, not only when a specific case makes it necessary;
- DPAs have to be proactive, conducting preliminary audits and evaluating privacy and data protection impact assessments of new data controlling operations, and since such operations are based almost entirely on new data processing technologies, these investigations also need the participation of ICT experts (one organisation noted that independence and impartiality can only be ensured if the experts represent the DPA itself;

(1) frequently, (2) sometimes, (3) almost never, the majority of the audience voted for option 2. A panellist added that data controllers *can* mislead DPAs in such matters whenever they want but they do this only infrequently, because they are afraid of the risks.

- involving the work of IT professionals is less expensive if those professionals are employed by the DPA.

Fig. 6. Developing own ICT expertise or importing from external sources



The reasons given by the few DPAs that preferred the use of external expertise were that:

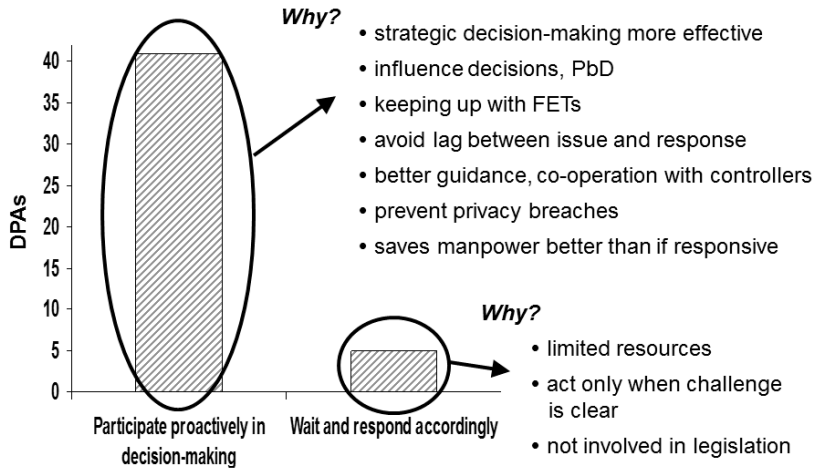
- external ICT experts may have a higher level of professional knowledge than those working at the data protection authorities;
- it is sufficient to involve IT professionals on a case-by-case basis, only when needed;
- in the case of small DPAs the size and the budget of the authority does not allow for the employment of in-house IT professionals.[13]

2.3. DPAs' strategies in ICT-related decision-making

Experience shows that DPAs, partly owing to the administrative and legal traditions of their respective countries, and partly to the traditions of the working methods they had developed over the years, lay different emphasis on the various tasks and roles we referred to in the Introduction of this article. This is also reflected in the way DPAs take part in ICT-related decision-making, including legislation, regulation, or giving opinions on certain data processing operations. The survey offered two options to the respondents: whether they prefer (a) participating proactively in strategic decision-making in privacy-related ICT matters, or (b) waiting until the real implications will be clear, and responding accordingly.

Fig. 7. Proactive or responding strategies

[13] The difference of opinion of the audience in the public discussion was even more pronounced: only one participant preferred the option of importing ICT expertise from external sources; all the other participants voted for developing such expertise inside the DPAs' offices.



Almost all DPAs preferred the proactive strategy, and only a few organisations preferred the reactive approach (Fig. 7). Among the reasons supporting proaction, the following deserve the most attention:

- DPAs' influence on strategic decision-making is more effective if performed proactively, particularly for promoting the application of the Privacy by Design;
- it is easier for the authorities to be involved in the development and application of future and emerging technologies (FETs) proactively;
- DPAs can avoid a disadvantageous lag between issue and response;
- the authorities can provide timely guidance to data controllers and establish useful co-operation with them, thereby preventing privacy breaches;
- proactive participation saves manpower better than does responsive action.

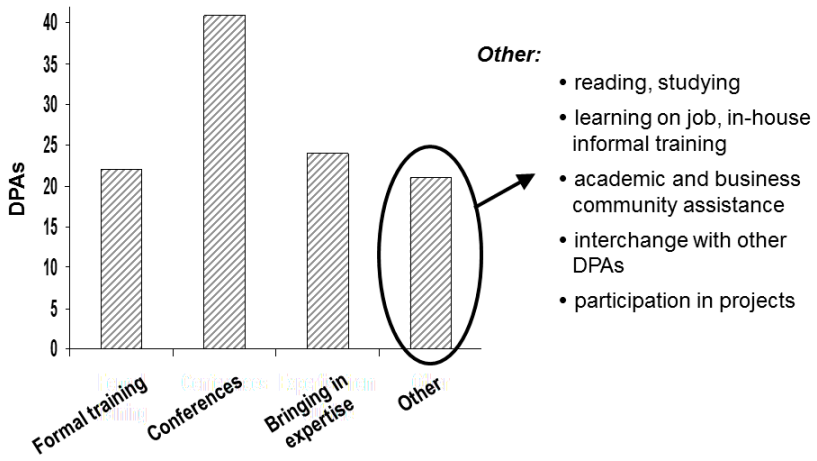
The few DPAs that preferred reactive actions mentioned their limited resources, or the fact that their organization is not involved in the legislative process, however, one DPA clearly stated that the proper strategy is to act only when the challenge is clear.[14]

2.4. DPAs' preferred ways to keep up with new developments

Although we did not ask DPAs opinion on the relevance of following new developments in information technology and understanding their implications in the area of privacy and data protection, we did ask a question about the methods DPAs prefer in acquiring this knowledge, with special regard to understanding FETs.[15] As can be seen in Fig. 8, respondents indicated a range of options, attending conferences and learning sessions being the most popular.[16]

Fig. 8. Keeping up with new developments in ICT

[14] The public discussion also revealed a sort of 'proaction paradox': despite the majority opinion on the importance of proactive strategies, DPAs do not seem to act proactively in many cases.
[15] Respondents could choose one or more options.
[16] Since the presentation of the survey findings and the public discussion also took place at a conference, this self-reflective discussion can be regarded as an indirect corroboration of this opinion.



The second most popular method was 'bringing in expertise from outside when necessary': more than twenty DPAs preferred this option. This seems to be somewhat contradictory to the opinions expressed in the issue of developing expertise in-house v. importing expertise from external sources, when only five responding authorities were in favour of the latter alternative. The results lead us to conclude that DPAs clearly distinguished the two situations: the importing of external expertise in investigations, and the importing of external expertise for educational purposes. Formal training was also among the popular options, and the respondents mentioned a range of other methods as well; for example:

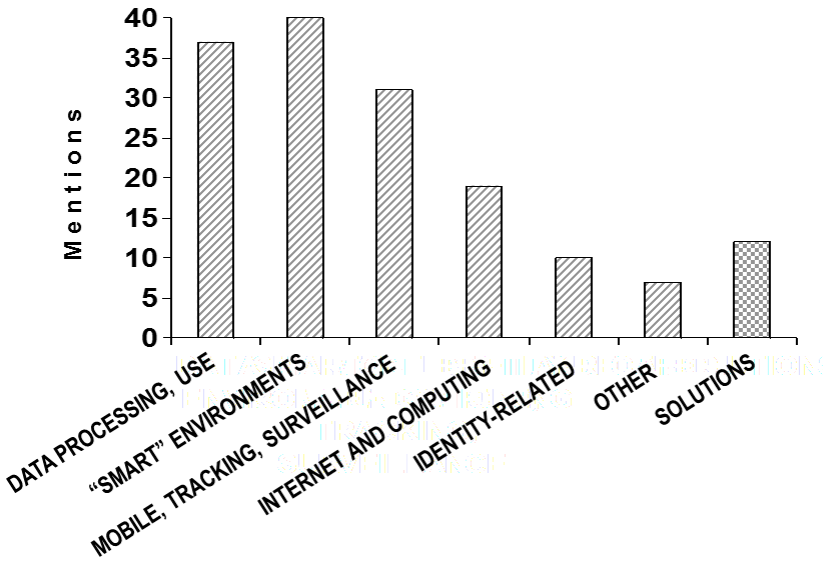
- individual self-development, such as reading professional literature or taking courses;
- learning while doing, i.e., acquiring the necessary knowledge on the job;
- organising in-house informal training sessions;
- asking or accepting assistance from the business or the academic community;
- exchange of experience and expertise with other DPAs;
- participation in research projects at the intersection of data protection and technology. [17]

2.5. The most important technologies: everything?

The last question of the survey addressed the issue of key technologies and applications, which are likely to have a significant impact on the privacy and data protection landscape in the foreseeable future. We asked DPAs to say which technologies or applications they thought will have the most significant impact on privacy in general, and on DPAs' activities and responsibilities in particular. We expected the frequent mentioning of well publicised technologies/applications such as big data analysis or the internet of things, along with a few country-specific ones. To our surprise, respondents mentioned an extremely wide range of technologies: there was no consensus on what technologies or applications will have the strongest impact on people's privacy and the DPAs' activities. The 43 authorities who responded to this question, altogether mentioned 68 technologies, applications or use cases, of which 62 could be regarded as 'risks' and 6 as 'solutions'.[18]

[17] PHAEDRA II (Barnard-Wills 2017) also reports some of these methods.
[18] Respondents could mention any number of technologies they found important. There were 152 mentions altogether; this means that one technology was mentioned only 2.2 times on average. The individual DPAs

Fig. 9. Relevant privacy-related technologies



In order to structure the responses, we set up categories and tried to classify each of the 68 technologies in one of these (Fig. 9). Although any new or emerging ICT or application may have relevance in virtually any of the categories, we classified the technologies according to their strongest real or perceived impact. Technologies relating to 'smart' environments were mentioned most frequently, followed by technologies influencing the general use and processing of personal data; mobile communication, tracking and surveillance constituted the third most popular category.[19]

3. Conclusion

The survey findings and the public discussion shed light on the fact that European data protection authorities regard the importance of this area differently, due to the different nature of their investigations, their different approaches to influencing developments in data processing technologies, and the differences in their available resources. In the public discussion, one of the panellists raised the idea of exchanging specific ICT expertise among DPAs by setting up a centre where such experts from DPAs' offices are registered and DPAs could exchange such experts for a limited time period. Such a centre could be an extension of the European Data Protection Board which is to be set up under the provisions of the GDPR. Another panellist replied to the moderator's question and noted the absence of a benchmark: it is difficult to evaluate even one's own expertise without such a benchmark, and makes the comparison between DPAs debatable.

Among the panel's audience, a representative of a large IT company expressed the view that it is not technology *strictu sensu* but technology and business practices together that needs to form part

mentioned 3.5 technologies on average. Barnard-Wills (2017: 143-144) highlights examples of three technologies or areas for technology foresight: big data, drones, and the Internet of Things.

[19] A panellist expressed the opinion that it is not the visible, high-risk technologies and applications which represent the real risks in data protection but the seemingly low-risk but generally applied technologies in developing applications for a wide community of users.

of the necessary expertise in the offices of the DPAs, and underlined the importance of establishing co-operation between DPAs and business entities or the industry as a whole. The panellists emphasised the importance of involving representatives from industry in discussions of new data-processing and -analysis technologies and their impact on privacy and data protection. However, they also warned that the moderation of such discussions should not be offered to the industry because business organisations have different motivations and value systems from those of DPAs.[20]

This article has only considered one aspect of the multiplex role of DPAs, perhaps most closely related to their 'expert knowledge', in Flaherty's (1997) terms: their knowledge of ICTs. It is not necessary here to rehearse or document the cliché that we live in an age of extremely rapid technological innovation, and of corporate and governmental use as well as popular dissemination of information-processing instruments and practices. Taking that as given, it characterises the world that powerfully shapes the performance – and the degree of success – of the multiple roles played by DPAs as among the official guardians of our personal data and our privacy, and of the wider societal interest in privacy as a public good (Regan, 1995; Raab, 2012). Flaherty (1998: 177) argues that '[o]ne cannot regulate a system without fully understanding it'; at issue here is the extent of DPAs' 'expert knowledge'. Meeting in London in 2006, the 28th International Conference of Data Protection and Privacy Commissioners adopted the 'London Initiative' that identified a number of challenges to individual liberties and to DPAs arising from the pace of technological change. These were: acceleration, globalisation, ambivalence, unpredictability, invisibility, and irreversibility.[21] The Conference also issued a final communiqué that included the following exhortation:

> **Commissioners should reinforce their capacities in technological areas**, with a view to advanced studies, expert opinions and interventions, in close interaction with research and industry in the field of new technology, and share this work together. The excessively 'legal' image of data protection must be corrected.[22]

In this spirit, it is worth noting that one of the GDPR's designated tasks (Article 57(1)(i) requires DPAs 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'. Moreover, most of the other tasks require decisions that would be based, in some part, upon the application of such technical and processing-systems knowledge to an array of subjects and practices covered under many other Articles. The adequacy of DPAs' cognitive capability regarding ICTs is likely to become increasingly questioned, and there are signs that many DPAs themselves have sought to take steps towards becoming better equipped than they have been in previous years. [23]

---

[20] A member of the audience, during the discussion of the survey findings, publicly offered to help in clarifying the impact of new and emerging technologies, if invited by a DPA. According to this intervention, such an earlier invitation by the Dutch data protection authority was very useful for both parties.

[21] Communicating Data Protection and Making it More Effective', available at: http://194.242.234.211/documents/10160/10704/Communicating+Data+Protection+and+Making+It+More+Effective.pdf, pp. 2-3.

[22] Closing Communiqué, 28th International Conference of Data Protection and Privacy Commissioners, 2nd and 3rd November 2006, London, United Kingdom, available at: https://edps.europa.eu/sites/edp/files/publication/06-11-03_london_communique_en_0.pdf; p. 5 (emphasis in original).

[23] See the proposals for co-operative and participatory ways forward for EU DPAs in undertaking technological foresight in PHAEDRA II (https://www.linkedin.com/pulse/phaedra-ii-project-data-protection-

Data protection in general, and the necessary ICT expertise in particular, are moving targets – in other words, there is no ideal state in data protection: rather, it can be regarded as a continuous process of learning. This is true for the designers of ICT systems processing personal data, the data controllers, the data subjects, and naturally the DPAs alike. Expertise in ICTs is crucial in this process, as the importance of existing new technologies and the foreseeable importance of future and emerging technologies are likely to increase. Therefore developing such expertise, and keeping up with new developments, is a core necessity for DPAs. This involves innovation in the means and methods they apply in order to be, or to remain, up to date in this field and effective in all their regulatory tasks.

Acknowledgements

The authors are grateful to the organisers of the 2016 Computers, Privacy and Data Protection (CPDP) Conference, to the panelists who took part in the panel on Data Protection Authorities and Technology, and to those who responded to the survey conducted among data protection authorities of the European Union.

References

Bamberger, K. and Mulligan, D. (2015) *Privacy on the Ground: Driving Corporate Behavior in the United States and Europe.* Cambridge, MA: The MIT Press.

Barnard-Wills, D. (2017) 'The technology foresight activities of European Union data protection authorities', *Technological Forecasting & Social Change,* 116: 142–150.

Bennett, C. and Raab, C. (2006) *The Governance of Privacy: Policy Instruments in Global Perspective.* Cambridge, MA: The MIT Press.

Bieker, F. (2017) 'Enforcing Data Protection Law – The Role of the Supervisory Authorities in Theory and Practice', in Lehmann, A., Whitehouse, D., Fischer-Hübner, S., Fritsch, L. and Raab, C. (eds.) *Privacy and Identity Management: Facing Up to Next Steps.* (11th IFIP WG 9.2, 9.5, 96/11.7, 11.4, 11.6/SIG 9.2.2 International Summer School) Karlstad, Sweden, August 21-26, 2016, Revised Selected Papers, Springer: 125-139.

Jóri, A. (2015) 'Shaping vs applying data protection law: two core functions of data protection authorities', *International Data Privacy Law*, 5, 2: 133-143.

Flaherty, D. (1998) 'Controlling Surveillance: Can Privacy Protection Be Made Effective?', in Agre, P. and Rotenberg, M. (eds.) *Technology and Privacy: The New Landscape.* Cambridge, MA: The MIT Press: 167-192.

Flaherty, D. (1989) *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States*. Chapel Hill, NC: University of North Carolina Press.

Hijmans, H. (2016) *The European Union as Guardian of Internet Privacy: The Story of Art 16 TFEU.* Springer.

---

authority-final-barnard-wills; http://www.phaedra-project.eu/deliverables-2/) and Barnard-Wills (2017:147-149).

Raab, C. (2012) 'Privacy, Social Values and the Public Interest', in Busch, A. and Hofmann, J. (eds.) 'Politik und die Regulierung von Information' ['Politics and the Regulation of Information'], *Politische Vierteljahresschrift* Sonderheft 46, Baden-Baden: Nomos Verlagsgesellschaft: 129-151.

Regan, P. (1995) *Legislating Privacy: Technology, Social Values, and Public Policy.* Chapel Hill, NC: University of North Carolina Press.

Schütz, P. (2012) 'Comparing formal independence of data protection authorities in selected EU Member States', Paper for the 4th Biennial ECPR Standing Group for Regulatory Governance Conference.

Simitis, S. (1983) 'Data Protection – A Few Critical Remarks', in Council of Europe, *Legislation and Data Protection,* Rome.

Ivan Szekely, social informatist, is an internationally known expert in the multidisciplinary fields of data protection and freedom of information. Former chief counsellor of the Hungarian Data Protection ombudsman, Szekely is at present Senior Research Fellow of the Vera and Donald Blinken Open Society Archives at Central European University, associate professor at the Budapest University of Technology and Economics, and advisory board member of the Eotvos Karoly Policy Institute. His research interests and publications are focused on information autonomy, openness and secrecy, privacy, identity, surveillance and resilience, memory and forgetting, and archivistics.

Charles Raab is Professorial Fellow, University of Edinburgh; co-Director of the Centre for Research into Information, Surveillance and Privacy (CRISP); co-Chair, Independent Digital Ethics Panel for Policing (IDEPP) (UK); Faculty Fellow-elect, Alan Turing Institute (ATI) (UK) and member, ATI Data Ethics Group; Research on privacy, data protection, surveillance, regulation, privacy impact assessment, data protection authorities, 'smart' environments, security, democracy, accountability, identity. Publications include (with C. Bennett), *The Governance of Privacy* (2003; 2006); (with B. Goold), *Protecting Information Privacy* (2011); (with Surveillance Studies Network), *A Report on the Surveillance Society* (2006; *Update Report* 2010); (with W. Webster *et al*, eds.), *Video Surveillance* (2012). Evidence to UK parliamentary committees (e.g., Intelligence and Security Committee of Parliament, 2014; House of Lords European Union Committee, Sub-Committee F, 2014); Specialist Adviser, House of Lords Constitution Committee for inquiry, *Surveillance: Citizens and the State*, HL Paper 18, Session 2008-09. Fellow, Academy of Social Sciences; Fellow, Royal Society of Arts.

Appendix A
The Questionnaire

Survey on Data Protection Authorities and technology

September 2015

Q 1. In your opinion, to what extent do DPAs *in general* have expertise regarding information and communication technologies (ICT)?

1	2	3	4	5	6	7	8	9	10
Low									High

Q 2. To what extent does *your organisation* have expertise in, or significant familiarity with, ICT?

1	2	3	4	5	6	7	8	9	10
Low									High

Q 3. How many people are on the staff of your DPA in regulatory, policy, legal, investigatory or management positions?

.....

Q 4. What proportion of *these members of your staff* have expertise in, or significant familiarity with, ICT?

- ☐ 0 – 10%
- ☐ 11 – 25%
- ☐ 26 – 50%
- ☐ More than 50%

Q 5. Are you satisfied that this proportion is sufficient for the work of your DPA?

- ☐ Yes
- ☐ No

If 'yes', please go to Q 7

Q 6. If you think it is not sufficient, what are the causes of the shortfall?
(choose one or more boxes)

- ☐ difficult to find qualified staff
- ☐ budget limitations
- ☐ other (please specify) .....

Q 7. Do you prefer:

- ☐ developing your own technical expertise within the DPA, or
- ☐ importing technical expertise from external sources when needed?

Why? .....

Q 8. What percentage of your organisation's investigations (responding to data subjects' complaints or initiated by the DPA itself) involve ICT-related aspects (e.g. the use of computerized databases or the Internet)?

.....%

Q 9. What percentage of your organisation's investigations (responding to data subjects' complaints or initiated by the DPA itself) require specific ICT expertise?

.....%

Q 10. How does your organisation keep up with new developments in ICT, with special regard to understanding future and emerging technologies (FETs)?
(choose one or more boxes)

- ☐ Formal or academic training/certification
- ☐ Attending conferences or learning sessions
- ☐ Bringing in expertise from outside when necessary
- ☐ Other (please specify): .....

Q 11. What do you as a DPA regard as more important:

- ☐ to participate proactively in strategic decision-making in privacy-related ICT matters, or
- ☐ to wait until the real implications will be clear, and respond accordingly?

Why? .....

Q 12. In your opinion, which technologies or applications will have the most significant impact on privacy in general, and on the DPA's activities and responsibilities in particular?

.....

Thank You!

Appendix B
The most important technologies mentioned by survey respondents (Q 12)

1. DATA PROCESSING, USE (37)

Big Data (18)
Profiling (3)
Predictive Profiling (2)
Analytics Tools (1)
Behavioral advertisements (1)
Big databases (1)
Data exchange technologies (1)
Deep learning (1)
E-commerce (1)
eGov applications (1)
File-sharing (1)
International transfers (1)
Internet for direct marketing (1)
PII data flows (1)
Scoring (1)
The data controller's attitude (1)
The massive data gathering from Internet use and connected devices (1)

2. INTERNET OF THINGS, 'SMART' ENVIRONMENTS AND TECHNOLOGIES (40)

Internet of Things (6)
Pervasive/ubiquitous computing (3)
Sensor technology (3)
Smart devices (3)
Smart cities and smart homes (2)
Smart grid (2)
Smart metering (2)
Connected things (2)
Autonomous cars (1)
Cloud of Things (1)
Industry 4.0, incl. Network Technologies (1)
Robotics (1)
Smart Systems (1)
Smart video analytics (1)
Totally new ecosystem (1)

3. MOBILE, COMMUNICATIONS, TRACKING, SURVEILLANCE (31)

Drones (6)
Location based and/or tracking services (5)

Mobile Applications for Smartphones (4)
Video surveillance (3)
GPS (2)
iBeacons and BLE Beacons (2)
Mobile and cloud-based computing (2)
Internet and mobile devices (smart phones etc.) (1)
Mobile devices (1)
RFID/NFC (1)
Tracking Technologies on Websites and Smartphones (1)
Wearable computing (1)
NSA tools (1)
Mobile communications (1)

4. INTERNET AND COMPUTING (9)

Social Networks (6)
Search engines (3)
Cloud Computing (6)
Cyber security (1)
ICT Security (1)
Online media (1)
WiFi (1)

5. IDENTITY-RELATED (10)

Biometrics (6)
Authentication and Identification technologies (2)
Genetics (1)
Identity thefts (1)

6. OTHER (7)

All technologies & applications that are part of standard development tools (1)
Broadly used ICT (1)
In general telematics (1)
Publication of videos (1)
Technologies or applications that do not inform users (1)
The one that will be used the most (1)
There are numerous threats: it is not possible to identify one (1)

SOLUTIONS (12)

Privacy by Design technologies and applications (4)
ITIL, PRINCE2 etc. (2)
Privacy Impact Assessment, DPIA (2)
Consumer Protection (1)
Cryptography as safeguard for security & privacy (1)
GDPR (1)

PETs (1)