CHAPTER 5
Precaution and privacy impact assessment as modes towards risk governance

David Wright, Raphaël Gellert,
Serge Gutwirth & Michael Friedewald

Introduction

A key objective of the PRESCIENT project is to develop a privacy impact assessment.[1] This paper describes some of the PRESCIENT consortium's considerations towards that end.

A privacy impact assessment can be seen as a tool for responsible research and innovation (RRI). RRI can be defined as a "transparent, interactive process by which societal actors and innovators become mutually responsive to each other with a view on the (ethical) acceptability, sustainability and societal desirability of the innovation process and its marketable products in order to allow a proper embedding of scientific and technological advances in our society".[2] Such a definition is close to how one could define privacy impact assessment (PIA), i.e., PIA is a process of engaging stakeholders in order to consider how privacy might be impacted by the development of a new technology, product, service, project or policy and what measures could be taken to avoid or mitigate unwanted effects.

This paper contends that PIAs are an instrument of risk governance that should, therefore, be understood and implemented within the framework of the precautionary principle. Precaution is the best theoretical framework of action in the face of uncertain risks. After considering the precautionary principle from a conceptual point of view, this paper goes on to discuss privacy impact assessment in practice and concludes with the possibility of the integration of PIA within the context of risk governance. The paper also offers comments on the notion of balancing privacy and other values.

The precautionary principle

The precautionary principle was born from a turn in the societal discourse over the effects of technological and scientific development. Indeed, as illustrated by the Chernobyl catastrophe, it became clear that technical progress could also equate to danger for human health and the environment.[3] It is in this respect that sociologist Ulrich Beck coined the term "risk society" to designate modern societies, since the latter are characterised by a public debate largely focused on the management of technology-derived risks.[4]

As evidenced by Dominique Bourg, the nature of technical progress as such has changed over the second half of the 20th century. Technical innovation has dramatically increased,

1 The PRESCIENT (Privacy and Emerging Sciences and Technologies) project is funded under the EU's Seventh Framework Programme for research and technological development (SIS-CT-2009-244779). For an overview of the PRESCIENT project, see Friedewald, Michael, David Wright, Serge Gutwirth and Emilio Mordini, "Privacy, data protection and emerging sciences and technologies: towards a common framework", *Innovation - The European Journal of Social Science Research*, Vol. 23, No. 1, March 2010.

2 See René von Schomberg's introduction to this volume. The notion of RRI was coined in the context of the Frontiers Technology Assessment Network of Excellence. See, for instance, Robinson, Douglas K.R., "Co-evolutionary scenarios: An application to prospecting futures of the responsible development of nanotechnology", *Technological Forecasting and Social Change*, Vol. 76, No. 9, November 2009, pp. 1222-1239.

3 Hilty, Lorenz M., Siegfried Behrendt, Mathias Binswanger et al., "The Precautionary Principle in the Information Society: Effects of Pervasive Computing on Health and Environment", TA 46e/2005, TA-Swiss, Centre for Technology Assessment, Bern, 2005. http://www.ta-swiss.ch/www-remain/reports_archive/publications/2005/050311_STOA125_PvC_72dpi_e.pdf. .

4 Beck, Ulrich, *Risk society – towards a new modernity*, Sage, London, 1992; Godard, Olivier, "Le principe de précaution, une nouvelle logique de l'action entre science et démocratie", *Philosophie Politique*, No. 11, May 2000, p. 21.

due to the correlative restless multiplication of new fields of knowledge and expertise. This, in turn, has created a situation where there is no complete mastery of the effects and/or consequences of such innovation. This situation, which differs from the one where all the causes and consequences concerning a particular technique are (thought to be) known, has paved the way to a phenomenal world that is characterised by the inadequate awareness of the effects and consequences of a particular technique; in other words, that is characterised by unpredictability and *uncertainty*.[5]

Such a shift from a situation wherein well-defined risks that could trigger a carefully planned course of actions (in line with the "principle of prevention", i.e., known risks can be prevented)[6] to a situation wherein risks become potential and uncertain, draws the limit of danger aversion strategies apparent, and spurs the need for a new framework of action: the precautionary principle.

Definition

The precautionary principle has been enshrined in various international legal texts, such as the Rio Declaration,[7] the Treaty on the Functioning of the European Union (TFEU),[8] in the WTO Sanitary and Phytosanitary (SPS) Agreements[9] as well as in national legislation, such as the French Barnier Act of 1995,[10] or the French Constitution.[11]

A satisfying definition of the principle has been provided in the academic discourse, and it has been suggested European policy makers should use it. According to this definition, the precautionary principle is the principle whereby, "following an assessment of available scientific information, there are reasonable grounds for concern for the possibility of adverse effects but scientific uncertainty persists, provisional risk management measures based on a broad cost/benefit analysis whereby priority will be given to human health and the environment, necessary to ensure the chosen high level of protection in the Community and proportionate to this level of protection, may be adopted, pending further scientific information for a more comprehensive risk assessment, without having to wait until the reality and seriousness of those adverse effects become fully apparent".[12]

5 Bourg, Dominique, "Le principe de précaution: un moment particulier de la philosophie de la technique", Seminar 'Le principe de précaution. Comment le définir, comment le faire appliquer?', Université Libre de Bruxelles, 1999, *in* Godard, op. cit., p. 7.

6 Cf. de Sadeleer, Nicolas, *Les principes du pollueur-payeur, de prévention et de précaution. Essai sur la genèse et la portée de quelques principes du droit de l'environnement*, Bruylant, Brussels,1999.

7 Principle 15 of the UN Conference on Environment and Development (UNCED) in Rio de Janeiro 1992 (Rio Declaration).

8 Art. 191, 11, 114.3, and 168.1 of the TFEU.

9 WTO Agreement on the Application of Sanitary and Phytosanitary Measures (SPS), art. 5.7.

10 Barnier Act of 1995 on the reinforcement of the protection of the environment (95-101).

11 Environment Charter, art. 5.

12 Von Schomberg, René, "The Precautionary Principle and its normative challenges", *in* Fisher, E., Jones, J., and von Schomberg, R., (eds), *Implementing the Precautionary Principle: Perspectives and Prospects*, Cheltenham, UK and Northampton, MA, US: Edward Elgar, 2006, p. 47.

In other words, the precautionary principle should guide governments' actions in situations characterised by risks that are not constitutive of acute dangers. Its purpose is to minimise risks that are not presently acute but that may become evident only in the longer term, and hence to maintain a margin for future developments.[13]

Kourilsky distinguishes between potential risks (i.e., uncertainties) and proven risks (i.e., acute dangers). The former will trigger a government response based upon the precautionary principle, whereas the latter will lead to a decision taken in the framework of the danger aversion principle (i.e., prevention).[14] As Godard puts it, the precautionary principle aims not only at dangers and risks whose causes are undetermined, but whose very existence is problematic and not yet ascertained.[15]

Its scope of action has been historically associated to environmental and human health matters. However, this is not an exhaustive list, and the principle has now been extended to consumer protection policy, but also to broader societal issues, including that of changes in moral principles. In this respect, the use of the precautionary principle in matters of pervasive computing and its implications in matters of privacy and data protection appears as logical.[16]

Precaution as a principle for immediate action

In its judgment on the validity of the Commission's decision banning the exportation of beef from the United Kingdom due to fears of BSE transmission, the ECJ has ruled that, "where there is uncertainty as to the existence or extent of risks to human health, the institutions may take protective measures without having to wait until the reality and seriousness of those risks become fully apparent."[17]

The precautionary principle thus commands that, in the face of a potential or anticipated risk, action must be taken at the earliest possible stage.

As Latour points out, the precautionary principle breaks the traditional link between scientific knowledge and action. Whereas danger aversion (i.e., prudence or prevention) entails that no action be taken before a complete knowledge of a situation is reached, the precautionary principle requires immediate action, though based upon criteria other than the sole knowledge of the causes and consequences of the concerned phenomenon. In other words, by disjoining (or disentangling) political action and scientific expertise, the precautionary principle is a new mode of governmentality based upon the necessity

13 Hilty et al. 2005, p. 27

14 de Sadeleer, op. cit., *passim*; Kourilsky, Philippe, *Du bon usage du principe de précaution*, Odile Jacob, Paris, 2002, p. 51.

15 Godard, op. cit., p. 6.

16 Hilty et al., op. cit., p. 29.

17 Judgment on the validity of the Commission's decision banning the exportation of beef from the United Kingdom to reduce the risk of BSE transmission (Judgments of 5 May 1998, cases C-157/96 and C-180/96), ground 63.

to take swift actions and decisions in situations of uncertainty.[18] In this respect, the precautionary principle is a *principle of action*.[19]

Understanding precaution as a principle of action requires determining the kind of actions that can be taken. Some procedural principles can be of help in this respect, such as comparing the merits and costs of different approaches or the need to take provisional measures (i.e., measures that can be revisable according to the evolution of scientific knowledge).[20]

As the European Commission points out, "recourse to the precautionary principle does not necessarily mean adopting final instruments designed to produce legal effects".[21] On the contrary, the appropriate response in a given situation is the result of an eminently political decision that weighs the acceptable level of risk that can be imposed on society, considering the particular risk at hand. Hence, in the face of a potential risk, the decision not to take any action may also be a valid response. Equally, the funding of a research programme or the decision to inform the public of the possible dangers of a phenomenon are also part of this wide range of actions that can be taken under the precautionary principle.[22]

Precaution and participation

A last issue of particular interest (especially in the light of PIAs) concerns the participation of stakeholders, including the public, in the decision-making process.[23]

One can ask why citizens should contribute to decision-making in the framework of the precautionary principle. The key for understanding this lies partly in the need to compensate for the deficiencies of political representation. Indeed, political representation in so-called modern democracies is characterised by an asymmetrical exposure to risk: political decisions will first and foremost affect citizens. Therefore, citizens might eventually criticise political officials, not simply for the fact that decision-making in situations of uncertainty inherently carries an irreducible element of risk, but more particularly for the behaviour of such officials who, because of personal interest, turpitude or negligence, happen to engage in paternalistic attitudes that resort to lenient justification or even to the concealment of risk-creating decisions that might affect large parts of the population without the latter

18 Latour, Bruno, "Prenons garde au principe de precaution", *Le Monde*, 1 Jan 2000. http://www.bruno-latour.fr/presse/presse_art/008.html

19 Godard, op. cit., pp. 10-11.

20 Ibid., pp. 57-66. It is unsurprising that Callon et al. have resorted to the expression "measured action", to design decision-making in this framework. See Callon, Lascoumes and Barthe, op. cit., chapter 6.

21 European Commission, Communication from the Commission on the precautionary principle, COM(2000) 1 final, 2 February 2000, p. 15. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2000:0001:FIN:EN:PDF

22 Kourilsky, op. cit., pp. 57-66.

23 Ibid., pp. 75-76.

benefiting from them whatsoever.[24] In other words, citizens have the right to be associated with decisions that carry risk for them (which the current state of political representation doesn't always fully permit).

The question remains as to what level of participation citizens should be entitled. Should it be a "simple" right of information or a fully-fledged participatory right?

In order to answer this question, it is necessary to turn to another procedure governing the precautionary principle. This procedural principle is based upon the evidence that situations of uncertainty (i.e., potential risk) are not based upon a complete ignorance of the situation, but the incompleteness of knowledge re theses situations.[25] Therefore, it is crucial to take into consideration all points of view, even the views of a minority, in order to have as complete a picture of the situation as possible. It is in this respect that the European Commission has recommended that, "even if a scientific opinion is supported by a minority fraction of the scientific community, due account should be taken of their views."[26]

The link between such an all-encompassing approach towards risk knowledge and citizens' participation goes as follows. The so-called risk society results partly from an ever-increasing complexity of technical and scientific knowledge that has gone beyond our control. Hence, as Godard argues, our management of risk cannot solely be based upon scientific knowledge. Setting aside scientific rationality, however, doesn't mean cutting all links with reason to be replaced by a heuristics of fear, for example.[27] Rather, it consists in anchoring decision-making into a new rationality, based upon collective deliberation, which is better equipped than pure scientific expertise to deal with situations of uncertainty.[28]

We now turn our attention to privacy impact assessment, which can be seen, in some sense, as an exercise in precaution, but especially as a form of risk governance.

Privacy impact assessment

Several privacy impact assessment methodologies already exist – Australia, Canada, New Zealand, the UK and the US have developed PIA policies and guidelines. The ISO has produced a standard for PIAs in financial services.[29] Interest in PIAs in Europe is growing. The European Commission's Recommendation on RFID included an article which called upon Member States and industry "in collaboration with relevant civil society stakeholders" to develop a PIA framework for RFID to be submitted for endorsement to the Article 29 Data

24 Godard, op. cit., pp. 15-16.

25 Ibid., p. 15.

26 European Commission, 2000, p. 16.

27 As put forward by Jonas. See, Jonas, Hans, *Le principe de responsabilité. Une éthique pour la civilisation technologique*. Éditions du Cerf, Paris,1990.

28 Godard, op. cit., pp. 16-19, especially p. 19.

29 ISO 22307:2008: Financial services -- Privacy impact assessment, 16 Apr 2008. http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=40897

Protection Working Party within 12 months (i.e., by May 2010).[30] Industry duly drafted a PIA for RFID. Although the Art. 29 WP rejected the first draft[31], it eventually agreed a subsequent draft in February 2011.[32]

There are other indications of a growing interest in PIA. European Commission Vice-President Viviane Reding said in July 2010 that "Businesses and public authorities... will need to better assume their responsibilities by putting in place certain mechanisms such as the appointment of Data Protection Officers, the carrying out of Privacy Impact Assessments and applying a 'Privacy by Design' approach.[33]

The European Parliament, in its 5 May 2010 resolution on Passenger Name Records, said that "any new legislative instrument must be preceded by a Privacy Impact Assessment and a proportionality test".[34]

Finally, the European Commission has said it will examine the possibility of including in its new data protection framework "an obligation for data controllers to carry out a data protection impact assessment in specific cases, for instance, when sensitive data are being processed, or when the type of processing otherwise involves specific risks, in particular when using specific technologies, mechanisms or procedures, including profiling or video surveillance".[35]

The interest in PIAs is growing, in part because of the perceived benefits, among which the following have been commonly cited:

- Building public trust:
  - Identifying and managing risks – Undertaking a PIA will help industry and government to foresee what the media and the public will accept in regard to impacts on privacy. With the growth in data-intensity and increasing use of

30 European Commission, Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification, C (2009) 3200 final, Brussels, 12 May 2009. http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf

31 Article 29 Data Protection Working Party, Opinion 5/2010 on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications, Adopted on 13 July 2010. http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2010_en.htm

32 Art. 29 Data Protection Working Party, Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications, Brussels, Adopted on 11 February 2011.

33 Reding, Viviane, Vice-President of the European Commission responsible for Justice, Fundamental Rights and Citizenship, "Towards a true Single Market of data protection", SPEECH/10/386, Meeting of the Article 29 Working Party «Review of the Data protection legal framework» Brussels, 14 July 2010. http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/386

34 European Parliament, Resolution of 5 May 2010 on the launch of negotiations for Passenger Name Record (PNR) agreements with the United States, Australia and Canada. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2010-0144+0+DOC+XML+V0//EN

35 European Commission, A comprehensive approach on personal data protection in the European Union, Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, COM(2010) 609 final, Brussels, 4.11.2010. http://ec.europa.eu/justice/news/intro/news_intro_en.htm#20101104

privacy-intrusive technologies, the risks of a project or scheme being rejected by the public are increasing.
  - Avoiding loss of trust and reputation – A PIA will help an organization's reputation and avoid deploying a system with privacy flaws which attract negative attention from the media, competitors, public interest advocacy groups, regulators and customers. Retrospective imposition of regulatory conditions may put the entire project at risk. A PIA provides an opportunity to obtain commitment from stakeholders early on and to avoid the emergence of opposition at a later, more costly stage.
  - Providing a credible source of information to assuage alarmist fears and alerting the complacent to potential pitfalls.
  - Achieving a better balance among conflicting interests.
  - Improving public awareness and making available more information about an envisaged system, service or project.

- Complying with national and international regulations:
  - Avoiding unnecessary costs – By performing a PIA early, an organization avoids problems being discovered at a later stage, when the costs of making significant changes or cancelling a flawed project outright are much greater.
  - Imposing the burden of proof for the harmlessness of a new technology, process, service or product on its promoters.

- Avoiding risky investments:
  - Avoiding inadequate solutions – Solutions devised at a later stage are often not as effective at managing privacy risks as solutions designed into the project from the start. "Bolt-on solutions devised only after a project is up and running can often be a sticking plaster on an open wound."[36]
  - Understanding the perspectives of stakeholders – Inputs from stakeholders may lead to a better-designed project, the difference between a privacy-invasive and a privacy-enhancing project, and pre-empt possible misinformation campaigns by opponents.
  - Improving security of personal data and making life more difficult for cyber criminals.[37]

The PRESCIENT consortium is examining these different initiatives, particularly those of the above-mentioned countries, to identify the best features of existing PIAs and, based on those, to produce a framework that integrates those "best" features. As PIAs are used in several different countries, it's not surprising that there are some differences in the process – when they are triggered, who conducts the process, the reporting requirements, the scope, the involvement of stakeholders, accountability and transparency.

PIAs can be distinguished from compliance checks, privacy audits and "prior checking". A compliance check is to ensure a project complies with relevant legislation or regulation. A privacy audit is a detailed analysis of a project or system already in place which either confirms that the project meets the requisite privacy standards or highlights problems

36 The quote comes from: Information Commissioner's Office (ICO), Privacy Impact Assessment Handbook, Version 2.0, June 2009, chapter I. http://www.ico.gov.uk/for_organisations/topic_specific_guides/pia_handbook.aspx

37 These benefits have been adapted from the ICO PIA handbook, op. cit., and from Stewart, Blair, *Privacy Impact Assessment Handbook*, Office of the Privacy Commissioner, Auckland, June 2007.

that need to be addressed.[38] Another important term to distinguish in this context is "prior checking", which appears in Article 20 of the European Data Protection Directive and which says in part that "Member States shall determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof".[39]

While the approaches to privacy impact assessment are somewhat similar – i.e., the PIA process aims at identifying impacts on privacy before a project is undertaken – there are also important differences. In December 2007, the UK became the first country in Europe to publish a privacy impact assessment handbook. The Information Commissioner's Office (ICO) published a second version in June 2009.[40] Before publication of its PIA handbook, ICO commissioned a set of studies by some of the world's leading PIA experts, including Colin Bennett, Robin Bayley, Roger Clarke and Andrew Charlesworth.[41] They examined the PIA practices in Australia, Canada, Hong Kong, New Zealand and the US before making their recommendations. Thus, in some ways, the UK has one of the most advanced PIA methodologies. It is especially distinguished by its emphasis on engaging stakeholders at an early stage.

Because organisations vary greatly in size and experience, and as the extent to which their activities might intrude on privacy also varies, the ICO says it is difficult to write a "one size fits all" guide. Instead, it envisages each organization undertaking a privacy impact assessment appropriate to its own circumstances.[42]

The ICO says the privacy impact assessment process should begin as soon as possible, when the PIA can genuinely affect the development of a project. The ICO uses the term "project" throughout its handbook, but clarifies that it could equally refer to a system, database, program, application, service or a scheme, or an enhancement to any of these, or even draft legislation.

The ICO envisages a privacy impact assessment as a process that aims to:

- identify a project's privacy impacts,
- understand and benefit from the perspectives of all stakeholders,
- understand the acceptability of the project and how people might be affected by it,
- identify and assess less privacy-invasive alternatives,
- identify ways of avoiding or mitigating negative impacts on privacy,
- document and publish the outcomes of the process.[43]

38 Warren, Adam, Robin Bayley, Colin Bennett, Andrew Charlesworth, Roger Clarke and Charles Oppenheim, "Privacy Impact Assessments: International experience as a basis for UK Guidance", *Computer Law and Security Report*, Vol. 24, 2008, pp. 233-242.

39 European Parliament and the Council, Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Brussels, 24 Oct 1995.

40 Op. cit.

41 Bennett, Colin, Robin Bayley, Roger Clarke, and Andrew Charlesworth, "Privacy Impact Assessments: International Study of their Application and Effects", Report for the Information Commissioner's Office, United Kingdom, Linden Consulting, Inc., 2007. http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/lbrouni_piastudy_apph_eur_2910071.pdf

42 ICO PIA handbook, op. cit., p. 2.

43 ICO PIA handbook, op. cit., p. 7.

The PIA process starts off with an initial assessment, which examines the project at an early stage, identifies stakeholders and makes an initial assessment of privacy risks. The ICO has appended some screening questions to its handbook the answers to which will help the organization decide whether a PIA is required, and if so, whether a full-scale or small-scale PIA is necessary.

A full-scale PIA has five phases:

In the **preliminary phase,** the organisation proposing the project prepares a background paper for discussion with stakeholders, which describes the project's objectives, scope and business rationale, the project's design, an initial assessment of the potential privacy issues and risks, the options for dealing with them and a list of the stakeholders to be invited to contribute to the PIA.

In the **preparation phase,** the organisation should prepare a stakeholder analysis, develop a consultation plan and establish a PIA consultative group (PCG), comprising representatives of stakeholders.

The **consultation and analysis phase** involves consultations with stakeholders, risk analysis, identification of problems and the search for solutions. Effective consultation depends on all stakeholders being well-informed about the project, having the opportunity to convey their views and concerns, and developing confidence that their views are reflected in the outcomes of the PIA process.

The **documentation phase** documents the PIA process and outcomes in a PIA report, which should contain

- a description of the project,
- an analysis of the privacy issues arising from it,
- the business case justifying privacy intrusion and its implications,
- a discussion of alternatives considered and the rationale for the decisions made,
- a description of the design features adopted to reduce and avoid privacy intrusion and the implications of these features,
- an analysis of the public acceptability of the scheme and its applications.

The **review and audit phase** involves a review of how well the mitigation and avoidance measures were implemented.

Because projects vary greatly, the handbook also provides guidance on the kinds of projects for which a small-scale PIA is appropriate. The phases in a small-scale PIA mirror those in a full-scale PIA, but a small-scale PIA is less formalised and does not warrant as great an investment of time and resources in analysis and information-gathering. An important feature of the PIA as envisaged by ICO is that it should be transparent, accountable, include external consultation where appropriate, and make reports publicly available.

While the UK PIA is very sophisticated, it does fall short of the US requirement that government agencies publish their PIAs on their websites. In Canada, government departments are required to publish summaries of their PIAs. In both countries, government departments are required to include a PIA when making submissions for funding, to the Treasury Board in the case of Canada and to the Office of Management and Budget (OMB) in the case of the US.

In the UK, there is no such requirement. In Canada, if the Treasury Board (which is also the guardian of the PIA policy) does not find a PIA to be adequate, it can turn down funding until the government department improves the PIA. Also in Canada, unlike the UK, government departments are required to send a copy of the PIA to the Office of the Privacy Commissioner (OPC), and the OPC has the power to conduct an independent audit of the government departments' PIA practices – and it has done so, as has the Governmental Accounting Office (GAO) in the US. While ICO does not know who has carried out PIAs, the OPC has called for a central registry of all (government-performed) PIAs.

Issues of balancing

Another procedural principle concerning action in the framework of precaution requires actors to make cost/benefit analyses between the different courses of action (or inaction) possible, and the different values at stake.[44] As indicated above, PIAs also resort to this type of operation. Hence, there is a need to clarify what constitutes a sound proportionality (i.e., balancing) test.

The traditional position regarding the balancing of conflicting fundamental rights and/or values leads to a catch. According to this view, balancing consists in simply opposing two values; it assumes that supporting one interest *ipso facto* weakens the other, that it is only possible to uphold one at the expense of the other.[45]

Such a position, which might be coined as "weak balancing", loses sight of the broader context in which such choices operate: the democratic constitutional State. The mission of such a State is precisely to nurture a wide range of values and principles, some of which (e.g., privacy and security) conflict at times.

Therefore, the aim of any balancing is not to weigh one right against another, but more precisely, to *reconcile* the multiple values that constitute the backbone of the democratic State in such a way that it is possible to organise a *cohabitation* between them that is as respectful as possible of the principles of the democratic constitutional State. In other words, the point of striking a balance between two values (whose antagonism might be irreducible at some point) is to preserve and enforce both of them in the best possible way.

In this respect, lessons can be drawn from the system of the European Convention of Human Rights (ECHR). Within this system, some rights enshrined therein – among which

44 Kourilsky, op. cit., pp. 56-67. See also, European Commission, 2000, op. cit., pp.16-19, especially p. 17.

45 In most of its case law regarding article 8 of the Convention, the European Court of Human Rights has adopted such a stance. When assessing the conformity of measures breaching the right to privacy, it has either refused to undertake a balancing by expanding the legality criteria or, when it has undertaken a balancing, it has only considered the more formal part of the test embodied by the proportionality test, which supports a classical, "weak balancing" perspective, see *infra,* next paragraph. De Hert, Paul, and Serge Gutwirth, "Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalism in Action", in Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile de Terwangne and Sjaak Nouwt (eds.), *Reinventing data protection?*, Springer, Dordrecht, 2002, pp. 20-24; De Hert, Paul, "Balancing security and liberty within the European human rights framework. A critical reading of the Court's case law in the light of surveillance and criminal law enforcement strategies after 9/11", *Utrecht Law Review*, 2005, Vol. 1, No. 1, pp. 91-93.

is article 8 which hallows the right to privacy[46] – can only be derogated under certain conditions, namely, that the derogation must be foreseen by law, must respond to one of the legitimate aims listed in article 8.2 (in the case of privacy),[47] be necessary in a democratic society and be proportionate to the aim pursued.[48]

Although all conditions must be fulfilled for a measure to infringe upon article 8, the core of the balancing process lies in the last two parameters: the "necessity in a democratic society" and the proportionality criteria.[49]

The Convention also contains the elements for a better, stronger balancing, which are embodied in the "necessary in a democratic society" condition. This means that when weighing two values, one has to ask whether the proposed measure is acceptable from a constitutional viewpoint since it might harm the very essence of the fundamental right in balance. Rather than bluntly balancing two opposing rights, the question becomes: "How much erosion of a fundamental right is compatible with the democratic constitutional State?" (given that fundamental rights are an inherent part of the latter) or "In which society do we want to live?". Equally, such a substantial, value-loaded test should lead us to ask ourselves whether there are alternative measures that, although leading to the same result (the nurturing of a certain value), do not affect other potentially conflicting fundamental rights. In other words, is there a way to protect and enforce both values without loss at the fundamental rights level? Is there a way to enforce two conflicting values without encroaching upon either? [50]

Such a strong balancing is better equipped to achieve the necessary *reconciliation* or *cohabitation* that must prevail between (sometimes) conflicting values that lie at the heart of the social contract from which stems the democratic constitutional State.

Consulting and engaging stakeholders

A process for engaging and consulting with stakeholders should be put in place to help policy-makers, technology developers and project managers in ensuring that privacy issues

46 Article 8.1 states that "Everyone has the right to respect for his private and family life, his home and his correspondence."

47 i.e., "The interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".

48 Article 8.2 only foresees the three first conditions, but the Court of Strasbourg has added the last one through its case law. See, Van Gerven, W., "Principe de proportionnalité, abus de droit et droits fondamentaux", *Journal des Tribunaux*, 1992, pp. 305-309; Ganshof Van Der Meersch, W.J., "Propos sur le texte de la loi et les principes généraux du droit", *Journal des Tribunaux,* 1970, pp. 557-574 and pp. 581-596; Eissen, M.-A., "The Principle of Proportionality in the Case-Law of the European Court of Human Rights" in Macdonald, R. St J., F. Matscher and H. Petzold (eds.), *The European System for the Protection of Human Rights*, Martinus Nijhoff, Dordrecht, 1993, pp. 125-37, especially p. 127.

49 De Vries, Katja, Rocco Bellanova, Paul De Hert and Serge Gutwirth, "The German Constitutional Court Judgment on data retention: proportionality overrides unlimited surveillance (doesn't it ?)", in Serge Gutwirth, Yves Poullet, et al. (eds.), *Privacy and data protection: an element of choice*, Springer, Berlin, 2011 [forthcoming], pp. 14-15.

50 Ibid., p. 15.

are identified, discussed and dealt with, preferably as early in the project development as possible. Of course, companies are not obliged to be as "democratic" and participatory as governments in developed countries have to be. And the involvement of stakeholders in the development is notoriously difficult and costly even if the products, services or policies have the potential for intrusion on privacy or are ethically dubious. Furthermore, competition in the private sector, especially in the development and promotion of new products and services, often involves secrecy in the early stages.

Nevertheless, there are various reasons why project managers should engage stakeholders and undertake a consultation when developing new technologies or projects. For one thing, Article 41 of the Charter of Fundamental Rights of the European Union, entitled the right to good administration, makes clear that this right includes "the right of every person to be heard, before any individual measure which would affect him or her adversely is taken", which suggests that consultation with stakeholders is not only desirable but necessary.

But there are other reasons too. Stakeholders may bring new information that the policy-maker, technology developer or project manager might not have considered and may have some good suggestions for resolving complex issues.[51] Also, technology development is often too complex to be fully understood by a single agent, as Sollie and others have pointed out.[52] Palm and Hansson state that "It would be delusive to believe that technology developers are conscious of all the effects of their products. In many cases, negative side effects come as a surprise to technology developers themselves. If they could have anticipated the negative consequences, they would, in the vast majority of the cases, have done their best to avoid them out of social concern or for commercial reasons, or both."[53] Furthermore, by engaging stakeholders, project managers may avoid subsequent criticism about a lack of consultation. Engaging stakeholders before the project is implemented may be a useful way of testing the waters, of gauging the public's reaction to the project. In any event, "A central premise of democratic government – the existence of an informed electorate – implies a free flow of information."[54] Even if participation does not increase support for a decision, it may clear up misunderstandings about the nature of a controversy and the views of various participants. And it may contribute generally to building trust in the process, with benefits for dealing with similar issues in the future.[55]

51 Stern, Paul C., and Harvey V Fineberg (eds.), *Understanding Risk: Informing Decisions in a Democratic Society*, Committee on Risk Characterization, National Research Council, National Academy Press, Washington, D.C., 1996. See also Oudshoorn, Nellie, and Trevor Pinch, *How Users Matter: The Co-Construction of Users and Technology*, MIT Press, Cambridge, MA, 2003.

52 Sollie, Paul, "Ethics, technology development and uncertainty: an outline for any future ethics of technology", *Journal of Information, Communications & Ethics in Society*, Vol. 5, No. 4, 2007, pp. 293-306 [p. 302]. See also Moor, James H., "Why we need better ethics for emerging technologies", *Ethics and Information Technology*, Vol. 7, No. 3, Sept 2005, pp. 111-119 [p. 118]. Moor also supports better collaboration among ethicists, scientists, social scientists and technologists.

53 Palm, Elin, and Sven Ove Hansson, "The case for ethical technology assessment (eTA)", *Technological Forecasting and Social Change*, Vol. 73, Issue 5, June 2006, pp. 543-558 [p. 547].

54 US National Research Council, Committee on Risk Perception and Communications, *Improving Risk Communication*, National Academy Press, Washington, D.C., 1989, p. 9. http://www.nap.edu/openbook.php?record_id=1189&page=R1

55 Stern and Fineberg, op. cit., pp. 23-24.

The process of identifying, discussing and dealing with privacy (and other ethical) issues should be ongoing throughout the project and perhaps even after it has been implemented, if only because new issues may arise that were not evident at the outset of the project development. Moor has made this point: "Because new technology allows us to perform activities in new ways, situations may arise in which we do not have adequate policies in place to guide us." Ethical problems can be generated at any point, says Moor, "but the number of ethical problems will be greater as the revolution progresses".[56]

The process of engaging stakeholders in consideration of ethical issues that may arise from the development of a new technology or the new use of an existing technology or a new policy or programme is arguably as important as the result. While stakeholders can make a substantial contribution to the decision-making process, at the end of the day, however, it is the policy-maker or technology developer who must take a decision whether to proceed with the technology or to modify it or to build some safeguards into its use in order to accommodate the concerns raised by stakeholders. It is the policy-maker or technology developer alone who will be held accountable for the decision.

Conclusion: PIA as part of risk management

It is in the interests of policy-makers, technology developers and project managers to conduct impact assessments involving stakeholders interested in or affected by the technology, as early in the development cycle as possible in order to minimise risks that may arise once the technology is launched. In some sense, impact assessments (like a privacy impact assessment) can be regarded as a form of risk management.[57]

While some decision-makers may think engaging stakeholders is a hassle or risks delaying development, the benefits of engaging stakeholders are numerous and should outweigh any such thoughts. This engagement also responds to a democratic necessity: if the consequences of new technological developments – which were not yet visible at the moment of the elections – are uncertain, the taking of action and of risks is a question of collective decision-making, and thus becomes a political issue. In addition, stakeholders may have some information or ideas or views or values that the project manager had not previously considered. They may be able to suggest alternative courses of actions to achieve the desired objectives. They may be able to suggest some safeguards which would minimise the risks that might otherwise become apparent after a technology or service is launched. By engaging stakeholders, the technology developer has a better chance of minimising

56 Moor, 2005, op. cit.. In his paper, Moor proposes the following hypothesis, which he calls "Moor's Law: As technological revolutions increase their social impact, ethical problems increase."

57 Verbeek indirectly offers at least two reasons supporting an ethical impact assessment. Two forms of designer responsibility can be distinguished here. First, designers can anticipate the impact, side-effects and mediating roles of the technology they are designing. On the basis of such anticipations, they could adapt the original design, or refrain from the design at all. Second, designers can also take a more radical step and deliberately design technologies in terms of their mediating roles. In that case, they explicitly design behaviour-influencing or 'moralizing' technologies: designers then inscribe desirable mediating effects in technologies." Verbeek, Peter-Paul, "The moral relevance of technological artefacts", Paul Sollie and Marcus Düwell (eds.), *Evaluating new technologies: methodological problems for the ethical assessment of technology developments*, Dordrecht, Springer, 2009, pp. 63–79 [p. 70].

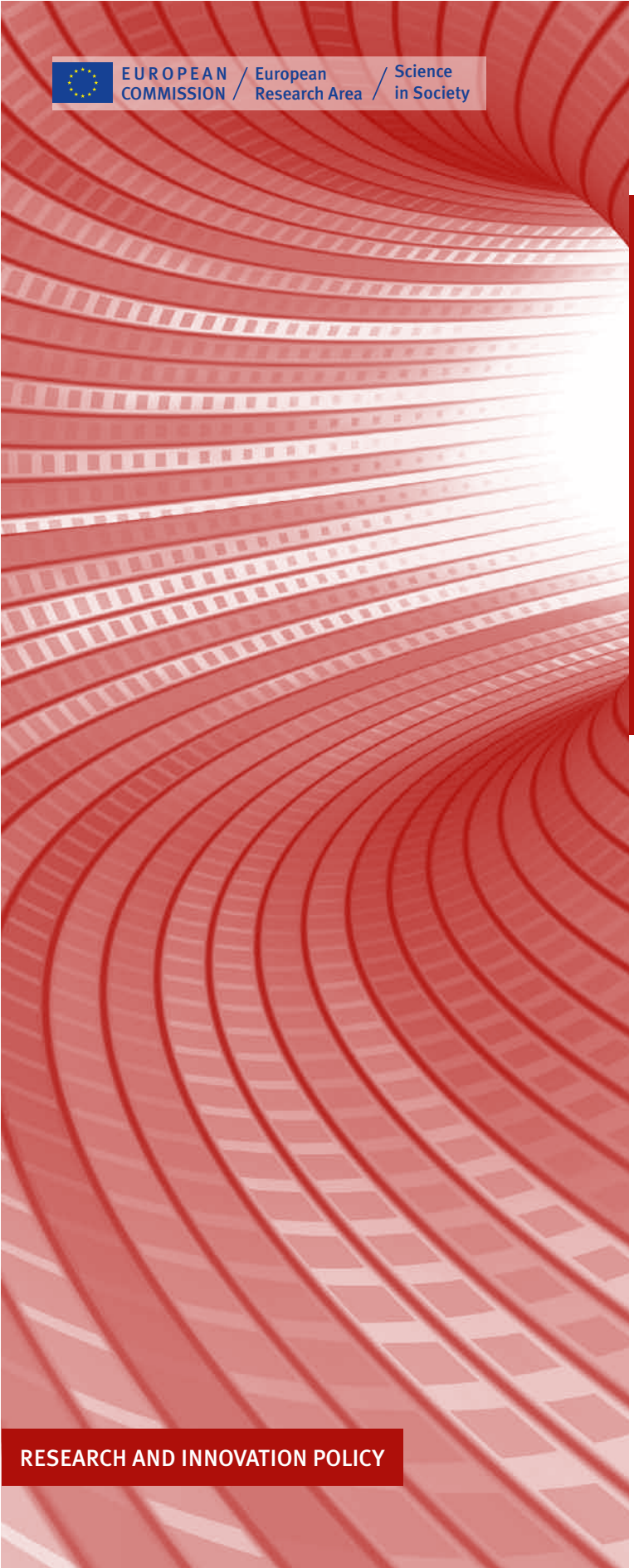
liability. The sooner stakeholders are brought into the process, the better. It will avoid subsequent criticisms and, possibly, costly retrofits downstream.

Many breaches in databases and losses of personal data held by government and industry have received a lot of negative publicity in the media. Undoubtedly, there are more breaches and losses that have not been reported by the media. Even so, those that have been reported take their toll in public trust and confidence. Most people simply do not believe their personal data is safe. There are justified fears that their personal data is used in ways not originally intended, fears of mission creep, of privacy intrusions, of our being in a surveillance society. Such fears and apprehensions slow down the development of e-government and e-commerce, and undermine trust in our public institutions.

As databases are established, grow and are shared, so do the risks to our data. A breach or loss of personal data should be regarded as a distinct risk for any organisation, especially in view of surveys that show most organisations have experienced intrusions and losses. Assuming that most organisations want to minimise their risks, then privacy impact assessments should be seen as a specialised and powerful tool for risk management. Indeed, PIAs should be integrated into the overall approach to risk management, and with other strategic planning instruments.[58]

In a society characterised by the unpredictability of risks that stem from existing as well from future and emerging technologies whose mastery is not totally in our hands, it is important to adopt a sound attitude towards those uncertainties that might have radical consequences. PIAs are a step in this direction. Practical issues such as how best to balance competing values, how best to implement such instruments at all pertinent levels and sectors of the society, or how to integrate stakeholders in the best participatory mode remain. However, this should not impede us from going towards an ethic of decision-making that relies upon its awareness of the radical uncertainty that characterises the world we live in, in order to better act with a view to preserving individual autonomy as well as the other fundamental values that underpin the democratic constitutional State.

58 Office of the Privacy Commissioner of Canada (OPC), Assessing the privacy impacts of programs, plans, and policies, Ottawa, October 2007. www.privcom.gc.ca



EUROPEAN COMMISSION / European Research Area / Science in Society

Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields

RESEARCH AND INNOVATION POLICY

EUROPE DIRECT is a service to help you find answers

to your questions about the European Union

Freephone number (*):

00 800 6 7 8 9 10 11

(*) Certain mobile telephone operators do not allow access to 00 800 numbers or these calls may be billed

Cataloguing data can be found at the end of this publication.

Luxembourg: Publications Office of the European Union, 2011

ISBN 978-92-79-20404-3
doi 10.2777/58723

Printed in France

PRINTED ON ELEMENTAL CHLORINE-FREE BLEACHED PAPER (ECF)

EUROPEAN COMMISSION

Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields

Edited by René von Schomberg[1]

A Report from the European Commission Services

1 Dr. René von Schomberg is based at DG Research and Innovation of the European Commission. This report is written for the publication series of the Ethics and Gender Unit of DG Research and Innovation. The views expressed here are those of the authors and may not in any circumstances be regarded as stating an official position of the European Commission.

2011 Directorate General for Research and Innovation

Table of contents

This publication, introduced and edited by René von Schomberg, consists of a series of research articles reflecting on how to proceed towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technology fields.

The authors who contributed to this publication are coordinators or participants to major FP7 projects funded under the Science in Society Programme. A total of 10 projects have inspired the authors to reflect and address various governance and ethics issues underlying the responsible development of these new technologies.

A deliberative approach to the responsible development of these technologies implies inclusive governance, based on broad stakeholder involvement, public debate and early societal intervention in research and innovation, among other, by means of ethics assessments and various technology and privacy impact assessments.

KI-NA-24835-EN-C

Publications Office

ISBN 978-92-79-20404-3