Winter 2011

Minimizing Technology Risks with PIAs, Precaution and Participation

Raphael Gellert, *Vrije Universiteit Brussel*
David Wright
Serge Gutwirth, *Vrije Universiteit Brussel*
Michael Friedewald, *Fraunhofer Institute for Systems and Innovation Research*

Minimizing Technology Risks with PIAs, Precaution and Participation

published in IEEE Technology and Society Magazine,
Vol. 30, No. 4, Winter 2011, pp. 47-54

David Wright, Raphaël Gellert, Serge Gutwirth & Michael Friedewald

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 [1]. 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.

In this light, PIA is also an instrument of risk governance that should, therefore, be understood and implemented within the framework of the precautionary principle. Precaution is a 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 that by integrating PIA within risk governance, one can also address the problem of balancing privacy and other values.

The precautionary principle

The precautionary principle was born from a turn in societal discourse over the effects of technological and scientific development. Indeed, the Chernobyl catastrophe (and, more recently, the catastrophe at the Fukushima nuclear power plant) made clear that technical progress poses dangers for human health and the environment [2]. In this regard, sociologist Ulrich Beck coined the term "risk society" to characterize modern societies, in which public debate is largely focused on the management of technology-derived risks [3, 4].

French philosopher Dominique Bourg has observed that the nature of technical progress as such has changed over the half century or so. Technical innovation has dramatically increased, due to 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 has paved the way to a world in which there is inadequate awareness of the effects and consequences of a particular technique, by unpredictability and *uncertainty* [4].

The shift from a situation wherein well-defined risks could trigger a carefully planned course of actions (in line with the "principle of prevention", i.e., known risks can be prevented) [5] to a situation wherein risks become potential and uncertain draws the

limit of apparent danger aversion strategies, and spurs the need for a new framework of action: the precautionary principle.

The precautionary principle has been enshrined in various international legal texts, such as the Rio Declaration (Principle 15 of the UN Conference on Environment and Development), as well as in national legislation.

Academic discourse has defined the precautionary principle, and when it can be applied, in in this way: "Where, 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… may be adopted… without having to wait until the reality and seriousness of those adverse effects become fully apparent" [6].

In other words, the precautionary principle should guide governments' actions in situations characterized by risks. Its purpose is to minimize 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 [2].

Philippe 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) [5, 7]. As Olivier 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 [4].

Its scope of action has been historically associated with environmental and human health matters. However, this is not an exhaustive list, and the principle has now been extended to consumer protection policy as well as to broader societal issues, including changes in moral principles. Thus, the use of the precautionary principle in matters of pervasive computing and its implications in matters of privacy and data protection appears logical [2], if not inevitable.

Precaution as a principle for immediate action

In its judgment on the validity of the European Commission's decision to ban the export of beef from the United Kingdom due to fears of BSE ("mad cow disease"), the European Court of Justice 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" (Judgments of 5 May 1998, cases C-157/96 and C-180/96, ground 63).

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

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 such a determination, 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 [4, 8].

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, the funding of a research programme or the decision to inform the public of the possible dangers of a phenomenon are among a range of actions that can be taken under the precautionary principle [7].

Precaution and participation

An issue of particular interest, especially in the light of PIA, concerns the participation of stakeholders, including the public, in the decision-making process [7].

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 characterized by an asymmetrical exposure to risk: political decisions will first and foremost affect citizens. Therefore, citizens might eventually criticize political officials, not simply for the fact that decision-making in situations of uncertainty inherently carries a risk, but more particularly for the behavior 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 benefiting from them whatsoever [4]. 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 to 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 regarding these situations [4]. 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..

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 [9]. 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 [4].

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

Privacy impact assessment

Several privacy impact assessment methodologies already exist – Australia, Canada, Ireland, New Zealand, the UK and the US have developed PIA policies and guidelines. The ISO has produced a standard for PIAs in financial services [10]. Interest in PIAs in Europe is growing as well.
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" [11].

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

A company or government department that undertakes a PIA with good intent, with a genuine interest in engaging stakeholders, including the public, has an opportunity of earning trust and good will from citizen-consumers. The extent to which it earns trust and good will will be a function of how open and transparent the organization makes the PIA process. The more open and transparent the process is, the more likely the organization is to overcome apprehensions, suspicions and mistrust in the development of a new service, product, policy, programme or project. Even if a new service does not engender public concerns (or those of privacy advocates), and there appears to be no mistrust to overcome, the organization can earn good will for being open and transparent about what it is planning to do. Businesses able to sustain a high level of trust and confidence can differentiate themselves from their rivals and thereby gain a competitive advantage [12].

By engaging stakeholders in the PIA process, an organization can benefit from ideas it may not have previously considered or it may find that stakeholders place much greater weight on some issues that the organization had regarded as relatively minor. If the project does raise difficult issues with regard to privacy, ideas from stakeholders may be particularly welcome. Even if stakeholders don't manage to generate some new considerations, the organization at least has an opportunity of gaining stakeholders' understanding and respect.

Transparency in the process may also be a way of avoiding liabilities downstream. If the organization is able to demonstrate that it did engage and consult with a wide range of stakeholders, was forthcoming with information, considered different points of view, it will be more difficult for some stakeholders to claim subsequently that the organization was negligent in its undertaking [13]. By being open and transparent from the outset, the organization can minimize the risk of negative media attention.

The New Zealand PIA Handbook describes a privacy impact assessment as an "early warning system". The PIA radar screen will enable an organization to spot a privacy problem and take effective counter-measures before that problem strikes the business

as a privacy crisis. It goes on to say that the PIA process can help the organization by providing credible information upon which business decisions can be based and by enabling organizations to identify and deal with their own problems internally and proactively rather than awaiting customer complaints, external intervention or a bad press [12].

PIA is a form of risk assessment, an integral part of risk management. It encourages cost-effective solutions, since it is less expensive to build "privacy by design" into projects, policies, technologies and other such initiatives at the design phase than attempt a more costly retrofit after a technology is deployed or a policy promulgated. Some simple adjustments may be all it takes to make the difference between a project that is privacy intrusive and one that has built in necessary safeguards. Thus, a PIA creates an opportunity for organizations to anticipate and address the likely impacts of new initiatives, to foresee problems and identify what needs to be done to design in features that minimize any impact on privacy and/or to find less privacy-intrusive alternatives.

A PIA should be regarded as a learning experience, for both the organization that undertakes the PIA as well as the stakeholders who are engaged in the process. An open PIA process helps the public understand what information the organization is collecting, why the information is being collected, how the information will be used and shared, how the information may be accessed, and how it will be securely stored [14]. The PIA's educational role is a way of demonstrating that the organization has critically analyzed how the project will deal with personal data. Where negative impacts on privacy are unavoidable, the PIA can help an organization decide whether those negative impacts are truly justifiable. Thus, a PIA thus promotes a more fully informed decision-making process [15].

PIA can be used to enforce or encourage accountability. A PIA should make clear who intends to do what and who will be responsible for what. It should make clear that, as a minimum, the project is fully compliant with privacy laws, regulations and relevant codes of conduct. If an executive knows he or she will be held accountable for a privacy-intrusive action, he or she may be less inclined to proceed with an action that seems likely to anger the public or, if not the general public, at least privacy advocates or other stakeholders likely to contest the action in the media.

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 that need to be addressed [16]. 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" [17].

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 [13]. Before publication of its PIA handbook, the 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 [18]. 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 organizations 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 [13].

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 [13].

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 Secretariat (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

Government Accountability Office (GAO) in the US. While the 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 [7, 19]. 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 [20, 21].

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 organize 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 is article 8 which hallows the right to privacy – 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), be necessary in a democratic society and be proportionate to the aim pursued [22-24].

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 [25].

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? [25]

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 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 [26, 27]. Also, technology development is often too complex to be fully understood by a single agent, as Sollie and others have pointed out [28, 29]. 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" [30]. 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" [31]. 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 [26].

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" [29].

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 ("privacy by design") 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 minimize 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. Verbeek [32] 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 behavior-influencing or "moralizing" technologies: designers then inscribe desirable mediating effects in technologies.

While some decision-makers may think engaging stakeholders is a hassle or risks delaying development, the benefits of engaging stakeholders are numerous, as indicated above, 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.

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 organization, especially in view of surveys that show most organizations have experienced intrusions and losses. Assuming that most organizations want to minimize their risks, then privacy impact assessments should be seen as a specialized and powerful tool for risk management. Indeed, PIAs should be integrated into the overall approach to risk management, and with other strategic planning instruments [33].

In a society characterized 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 characterizes 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.

Acknowledgement

This paper is based on research undertaken in the PRESCIENT (Privacy and Emerging Sciences and Technologies) project [34] funded under the European Commission's 7th Framework Programme for research and technological development (SIS-CT-2009-244779).

References

[1] D. K. R. Robinson, "Co-evolutionary scenarios: An application to prospecting futures of the responsible development of nanotechnology," in *Technological Forecasting and Social Change,* vol. 76, pp. 1222-1239, 2009.

[2] L. M. Hilty, S. Behrendt, M. 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, Berne, 2005.

[3] U. Beck, *Risk society – towards a new modernity*, London: Sage, 1992.

[4] O. Godard, "Le principe de précaution, une nouvelle logique de l'action entre science et démocratie," in *Philosophie Politique*, no. 11, pp. 17-56, May, 2000.

[5] N. de Sadeleer, *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*, Brussels: Bruylant, 1999.

[6] R. von Schomberg, "The Precautionary Principle and its normative challenges," in *Implementing the Precautionary Principle: Perspectives and Prospects*, E. Fisher, J. S. Jones and R. von Schomberg, Eds., Cheltenham, UK and Northampton, MA: Edward Elgar, 2006, pp. 19-41.

[7] P. Kourilsky, *Du bon usage du principe de précaution*, Paris: Odile Jacob, 2002.
[8] M. Callon, P. Lascoumes, and Y. Barthe, *Agir dans un monde incertain: essai sur la démocratie technique*, Paris: Seuil, 2001.
[9] H. Jonas, *Das Prinzip Verantwortung: Versuch einer Ethik für die technologische Zivilisation [1979]*, Frankfurt am Main, 1984.
[10] ISO 22307, *Financial services - Privacy impact assessment*, International Standardisation Organisation, Geneva, Switzerland, 2008.
[11] European Commission, *A comprehensive approach on personal data protection in the European Union,* COM(2010) 609 final, Brussels, 2010.
[12] B. Stewart, *Privacy Impact Assessment Handbook*, Office of the Privacy Commissioner, Wellington and Auckland, 2007.
[13] ICO, *Privacy impact assessment handbook. Version 2.0*, UK Information Commissioner's Office, London, 2009.
[14] Department of Homeland Security, *Privacy Impact Assessments: The Privacy Office Official Guidance*, Washington, DC, 2010.
[15] T. J. Karol, *A Guide To Cross-Border Privacy Impact Assessments*, Deloitte & Touche, Washington, D.C., 2001.
[16] A. Warren, R. Bayley, C. Bennett *et al.*, "Privacy Impact Assessments: International experience as a basis for UK Guidance," in *Computer Law and Security Report,* vol. 24, pp. 233-242, 2008.
[17] "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data on the free movement of such data," in *Official Journal of the European Communities,* vol. L 281, no. 23 November 1995, pp. 31-50, 1995.
[18] C. Bennett, R. Bayley, R. Clarke *et al.*, *Privacy Impact Assessments: International Study of their Application and Effects* Report for the Information Commissioner's Office, United Kingdom, Linden Consulting, Inc., 2007.
[19] European Commission, *Communication on the Precautionary Principle,* COM(2000) 1, Brussels, 2000.
[20] P. De Hert, and S. Gutwirth, "Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalism in Action," in *Reinventing Data Protection?*, S. Gutwirth, Y. Poullet, P. De Hert *et al.*, Eds., Dordrecht: Springer, 2009, pp. 3-44.
[21] P. De Hert, "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," in *Utrecht Law Review,* vol. 1, no. 1, pp. 68-96, 2005.
[22] W. Van Gerven, "Principe de proportionnalité, abus de droit et droits fondamentaux," in *Journal des Tribunaux*, pp. 305-309, 1992.
[23] W. J. Ganshof Van Der Meersch, "Propos sur le texte de la loi et les principes généraux du droit," in *Journal des Tribunaux*, pp. 557-574, 581-596, 1970.
[24] M.-A. Eissen, "The Principle of Proportionality in the Case-Law of the European Court of Human Rights," in *The European System for the Protection of Human Rights*, R. S. J. Macdonald, F. Matscher and H. Petzold, Eds., Dordrecht: Kluwer, 1993, pp. 125-137.
[25] K. d. Vries, R. Bellanova, P. De Hert *et al.*, "The German Constitutional Court Judgement on data retention: proportionality overrides unlimited surveillance (doesn't it ?)," in *Privacy and data protection: An element of choice*, S. Gutwirth, Y. Poullet, P. D. Hert *et al.*, Eds., Berlin: Springer, 2011, pp. 3-23.

[26] P. C. Stern, and H. V. Fineberg eds., “Understanding Risk: Informing Decisions in a Democratic Society,” Washington, D.C.: National Academy Press, 1996.
[27] N. Oudshoorn, and T. Pinch eds., “How Users Matter: The Co-Construction of Users and Technology,” Cambridge, Mass. and London: MIT Press, 2003.
[28] P. Sollie, “Ethics, technology development and uncertainty: an outline for any future ethics of technology,” in *Journal of Information, Communication & Ethics in Society,* vol. 5, no. 4, pp. 293-306, 2007.
[29] J. H. Moor, “Why we need better ethics for emerging technologies,” in *Ethics and Information Technology,* vol. 7, no. 3, pp. 111-119 September, 2005.
[30] E. Palm, and S. O. Hansson, “The Case for Ethical Technology Assessment (eTA),” in *Technological Forecasting and Social Change,* vol. 73, no. 5, pp. 543-558, 2006.
[31] National Research Council, Committee on Risk Perception and Communication, *Improving Risk Communication*, Washington: National Academies Press, 1989.
[32] P.-P. Verbeek, "The moral relevance of technological artefacts," in *Evaluating new technologies: methodological problems for the ethical assessment of technology developments*, P. Sollie and M. Düwell, Eds., Dordrecht: Springer, 2009, pp. 63–79.
[33] OPCC, *Assessing the Privacy Impacts of Programs, Plans, and Policies,* Audit Report of the Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada, Ottawa, 2007.
[34] M. Friedewald, D. Wright, S. Gutwirth *et al.*, “Privacy, Data Protection and Emerging Sciences and Technologies: Towards a common Framework,” in *Innovation: The European Journal of Social Science Research,* vol. 23, no. 1, pp. 63-69, March, 2010.