Science and Public Policy **40** (2013) pp. 755–766 doi:10.1093/scipol/sct083

Integrating privacy and ethical impact assessments

David Wright[1] and Michael Friedewald[2,*]

[1]*Trilateral Research & Consulting, Crown House, 72 Hammersmith Road, London W14 8TH, UK; Email: david.wright@trilateralresearch.com.*

[2]*Fraunhofer Institute for Systems and Innovation Research, Breslauer Strasse 48, 76139 Karlsruhe, Germany.*

**Corresponding author. Email: michael.friedewald@isi.fraunhofer.de.*

New and emerging technologies often raise both ethical and privacy issues. The analysis and assessment of such issues is the task of privacy impact assessments and ethical impact assessments. Although there are various privacy impact assessment methodologies and ethical impact assessment methodologies, the two have not been integrated. Nevertheless, some researchers have been thinking about the utility and feasibility of integrating privacy and ethical impact assessment methodologies.

Keywords: privacy; ethics; impact assessment; emerging technologies; data protection reform.

1. Introduction

In this paper we briefly review privacy impact assessments (PIAs) and ethical impact assessments (EIAs) and propose an integration of the two methodologies in line with the notion of responsible research and innovation (RRI). Thus, in Section 2, we outline the privacy challenges originating from emerging technologies and the various reactions in the EU policy arena to address them. In Section 3 we compare the different approaches towards PIA developed in five countries and the EU. In Section 4 we argue that PIAs and EIAs could follow similar processes, which lend themselves to their integration. Nevertheless, such integration faces certain challenges which are outlined here. The paper concludes that there are several reasons why such an integration is not only feasible, but also useful and merits the attention of policy-makers and project managers alike.

2. Policy background and challenges from emerging technologies

Especially in recent decades, science and technology have become driving forces in the development of our society. Consequently, in an open and democratic society, research is increasingly obliged to disclose and justify the rationale behind it. One element of the approaches to a governance of science is to:

> ... seek ways to enact basic fundamental rights of dignity, freedom, equality, solidarity, citizens' rights, and justice. (Ozolina et al. 2009: 7)

This is needed in research projects, especially publicly funded ones. When the EU Expert Group on Global Governance of Science wrote this recommendation in 2009, privacy impacts were not yet fully within the scope of policy-makers but were already recognised as future challenges. Since then, privacy has become an important topic in the work done or funded by the European Commission (EC). Many experts have commented on the difficulty of defining privacy.[1] Solove, a leading privacy scholar, has said that:

> ... privacy is a plurality of different things and that the quest for a singular essence of privacy leads to a dead end. There is no overarching conception of privacy—it must be mapped like terrain, by painstakingly studying the landscape. (Solove 2008: ix)

Not everyone sees the lack of an agreed definition as a problem. Finn et al. (2013: 26) have argued that:

> ... privacy is an inherently heterogeneous, fluid and multi-dimensional concept, and we suggest that this multidimensionality may be necessary to provide a platform from which the effects of new technologies can be evaluated. This potential necessity is supported by the fact that different technologies impact upon different types of privacy.

Even if privacy is difficult to define, it is nevertheless a fundamental right, protected by Article 7 of the Charter of Fundamental Rights of the EU. It is often regarded as an ethical issue as well, as reflected in a recent report of the European Group on Ethics in Science and New Technologies (EGE 2012). The PRESCIENT consortium, in which the authors of this paper were partners, commented on privacy and ethics as follows:

> When thinking in ethical terms about privacy, one has to remember that ethics is a branch of philosophy that assesses questions about morality; say about issues that can be classified as good (or right) and bad (or wrong) ... This implies that ethics will only be mobilized when there is the necessity to assess (or judge from a moral viewpoint) a course of action, undertaken by an autonomous agent. In our case, ethics thus relates to actions involving the privacy of individuals. Hence, ethics appears to be a procedural tool that provides guidelines in order to assess a selected course of action, but whose scope is not about giving a substantial definition of a notion. In other words, it can only assess actions relating to a pre-existing concept. Consequently, the scope of ethics lies more in trying to value the notion of privacy, rather than trying to substantiate it. Therefore, and in order to grasp this concept, ethics, as a branch of philosophy, naturally turns towards this discipline in order to provide a definition of privacy. (Gutwirth et al. 2011: 58)

One important point to derive from the above discussion is that privacy and ethics are somewhat intertwined. Privacy is both a fundamental right as well as an ethical issue. This intertwining makes it plausible, and even desirable or necessary, to assess privacy risks and ethical issues together. In addition to the intertwining of privacy and ethics, technology and privacy have also been two intertwined notions that must be addressed together.[2] Technology is a social practice embodying the capacity of societies to transform themselves by creating the possibility to create and manipulate not only physical objects, but also symbols, cultural forms and social relations. In turn, privacy describes a vital and complex aspect of these social relations. Thus, technology influences people's understanding of privacy, and people's understanding of privacy is a key factor in defining the direction of technological development. Either policy-making takes this rich and nuanced interplay between technology and privacy into account, or we run the risk of failing to govern the current, concomitant, technology and privacy revolution.

With the 'technology revolution(s)' of the last decades (ranging from the internet to genetics), the notion of privacy has started a new journey. For instance, there is R&D on information and communication technologies (ICT) implants, with which it becomes possible that a technologically 'enhanced' body communicates with nearby computers and exchanges data (Böhle et al. 2013). There are scientific development in genomics and proteomics that call for reconsidering the concept of 'personal information' (Taylor 2012), not to mention issues raised by technologies such as biometrics, smart surveillance systems and neurotechnology (Finn et al. 2011).

However, it becomes clear that many of the privacy problems produced by new technologies can no longer be adequately assessed and addressed with revised data protection approaches alone. With the advent of new technologies such as next-generation biometrics, DNA sequencing and human enhancement technologies, the data being collected moves from simply describing a person to being an inherent part of the person (Hallinan et al. 2013). All these challenges make it necessary not only to broaden data protection procedures and regulations but also to take other human values and rights into account to support policy-makers and decision-takers to better balance countervailing interests.

Since 2009, the EC has also promoted the concept of RRI which has gained increasing EU policy relevance (Owen et al. 2012; Stahl 2013). According to von Schomberg (2011: 50), RRI is a:

> ... transparent, interactive process by which societal actors and innovators become mutually responsive to each other with a view on the (ethically) acceptability, sustainability and societal desirability of the innovation process and its marketable products.

From these developments, it becomes clear that the assessment of privacy and ethical impacts of emerging technologies will be important building blocks of a holistic approach towards RRI, as outlined by von Schomberg (2013) and endorsed by the EU Expert Group on Ethical and Regulatory Challenges to Science and Research Policy (Ozolina et al. 2012).

The trends towards a broader and more integrated assessment of technology impacts is not only an element of RRI but was also discussed as an important element in the reform of the European data protection framework. The idea of PIA was taken up from Anglo-Saxon countries where PIAs had been developed and used since the early 1990s (Clarke 2009). As a first step, the EC (Directorate General INFSO, now Directorate General Connect) initiated the development of a PIA framework for radio frequency identification applications (Spiekermann 2012). At the same time, the Directorate General Justice explored national PIA schemes and good practice elements (Wadhwa and Rodrigues 2013). Finally, the EC included provision for a mandatory PIA (or data protection impact assessment, as the EC calls it) in its proposed Data Protection Regulation released in January 2012 (EC 2012: Art. 33).

It is thus a highly topical task to further develop methods and processes for an integrated assessment of technology impacts including privacy, ethics and others and to try to integrate them with an established way to assess and manage technology risks. This paper proposes a way to integrate PIAs and EIAs as an element of the future framework for the governance of emerging technologies.

3. Privacy Impact Assessment

PIA is a methodology for assessing the impacts on privacy of a project, policy, programme, service, product or other initiative and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimise negative impacts (Wright 2012: 55). PIA is gaining traction as an important instrument for protecting personal data and privacy. Several countries have been using PIAs, in some instances, for more than a decade. The countries with the most experience are: Australia, Canada, Ireland, New Zealand, the UK and the USA. While there are differences in the methodologies, all of them are concerned with identifying risks to privacy and finding ways of overcoming those risks. Sections 3.1–3.7 offer a thumbnail sketch of the principal PIA policies and methodologies.[3]

3.1 Australia

In Australia, the Office of the Privacy Commissioner (OPC) published its Privacy Impact Assessment Guide in August 2006, and a revised version in May 2010 (OAIC 2010). The Guide is addressed to government agencies, the private sector and the not-for-profit sector (i.e. civil society organisations). However, there is no legislative requirement in Australia to conduct a PIA. The Guide does not impose a particular PIA style ('There is no one-size-fits-all PIA model.') but suggests a flexible approach depending on the nature of the project and the information collected. The PIA Guide (OAIC 2010) says that:

> Consultation with key stakeholders is basic to the PIA process.

The Privacy Commission encourages organisations, 'where appropriate', to make the PIA findings available to the public.[4]

In Australia's Victoria state, the Office of the Victorian Privacy Commissioner (OVPC) has produced:

> . . . one of the three most useful guidance documents available in any jurisdiction, anywhere in the world. (Clarke 2012)

The current OVPC PIA Guide, dating from April 2009, is primarily aimed at the public sector in Victoria, but it says it may assist anyone undertaking a PIA. The Guide says that public consultation as part of the PIA process not only allows for independent scrutiny, but also generates confidence amongst the public that their privacy has been considered. Public consultation may generate new options or ideas for dealing with a policy problem. If wide public consultation is not an option, the Guide says the organisation could consult key stakeholders who represent the project's client base or the wider public interest or who have expertise in privacy, human rights and civil liberties (OVPC 2009).

3.2 Canada

In Canada, the Treasury Board Secretariat (TBS) issued PIA Guidelines in August 2002 (TBS 2002). It promulgated a new Directive on PIA in April 2010 (TBS 2010). The Directive ties PIAs with submissions to the Treasury Board for programme approval and funding. This is one of the strongest features of Canadian PIA policy. PIAs have to be signed off by senior officials, which is good for ensuring accountability, before a submission is made to the Treasury Board. The PIA is to be 'simultaneously' provided to the Office of the Privacy Commissioner, who has the power to audit PIAs. Institutions are instructed to make parts of the PIA publicly available. Exceptions to public release are permitted for security as well as 'any other confidentiality or legal consideration'.

In January 2009, the Office of the Information and Privacy Commissioner (OIPC) of Alberta issued a revised the PIA template and guidelines (OIPC 2009). Not only are PIAs mandatory for health care projects, they must be submitted to the OIPC before implementation of a new system or practice. If the OIPC finds shortcomings, projects can be turned down or forced to make costly retrofits.

3.3 Ireland

The Health Information and Quality Authority (HIQA) in Ireland produced a PIA Guidance in December 2010 (HIQA 2010b) following its review of PIA practice in other jurisdictions (HIQA 2010a), which found a growing convergence in what constitutes best practice in relation to PIAs. The HIQA favours the publication of PIA reports as it builds a culture of accountability and transparency and inspires public confidence in the service provider's handling of personal health information.

3.4 New Zealand

New Zealand's Office of the Privacy Commissioner (OPC) published a PIA Handbook in October 2002 (reprinted in 2007) (OPC 2007). It recommends that PIA reports be made publicly available, either in full or summary on an organisation's website. The Handbook mentions consultation with stakeholders but does not outline the consultative process. The agency conducting the PIA may consult the Privacy Commissioner. PIAs are generally not mandatory in New Zealand, however, section 32 of the Immigration Act 2009 explicitly requires PIA be conducted if biometric data are processed.

3.5 UK

The Information Commissioner's Office (ICO) in the UK published a PIA handbook in December 2007 and became the first country in Europe to do so. The ICO published a

revised version in June 2009 (ICO 2009) and a further revision in August 2013, a PIA code of practice, which was subject to public consultation until 5 November 2013. The Cabinet Office, in its Data Handling Review, called for all central government departments to:

> . . . introduce Privacy Impact Assessments, which ensure that privacy issues are factored into plans from the start. (Cabinet Office 2008a)

It stressed that PIAs will be used and monitored in all departments. PIAs have thus become a 'mandatory minimum measure' (Cabinet Office 2008b). The Handbook places responsibility for managing a PIA at the senior executive level (preferably someone with responsibility for risk management, audit or compliance). The ICO emphasises identification of, and consultation with, stakeholders.

3.6 USA

In the USA, PIAs for government agencies are mandated under the E-Government Act of 2002. Agencies are expected to provide their director with a copy of the PIA for each system for which funding is requested. On 26 Sept 2003, the Office of Management and Budget (OMB) issued a Memorandum to heads of executive departments and agencies providing guidance for implementing the privacy provisions of the E-Government Act (OMB 2003).

3.7 EU

Article 33 of the EC's proposed new Data Protection Regulation would make data protection impact assessments (otherwise known as PIAs) mandatory in cases:

> . . . where processing operations present specific risks to the rights and freedoms of data subjects.

In view of the hundreds of thousands of companies and government departments that process personal data across Europe, this provision could greatly increase the use of PIA in all countries in the EU—and beyond, especially where non-EU organisations sell products or provide services in Europe. Finally the Data Protection Regulation could serve as a template for third-state regulation; and so the PIA scheme that the EC will finally adopt could give momentum to the development of an international standard.

Article 33 briefly describes what a PIA report shall contain: 'at least' a general description of the envisaged processing operations, an assessment of the risks to data subjects, the measures envisaged to address those risks, safeguards, security measures and mechanisms to ensure the protection of personal data and should demonstrate compliance with the Regulation. Article 32a, as it emerged from the European Parliament's LIBE committee (Civil Liberties, Justice and Home Affairs) in October 2013, sets out data processing operations likely to present specific risks, e.g., processing of personal data relating to more than 5,000 data subjects, processing of special categories of personal data, location data or data on children or employees in large scale filing systems, profiling, processing of personal data for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases, automated monitoring of publicly accessible areas on a large scale, among other risks.

4. Ethical Impact Assessment

Much can be (and has been) learned from a review of these different methodologies in designing a more optimised approach to a PIA plus EIA (P+EIA), as will be discussed in Section 5. The Irish and UK PIA handbooks both are based on extensive reviews of other PIA methodologies. Hence, with promotion of the RRI concept and other forms for a more holistic technology assessment (TA) we can see a distinct evolution in enhancing PIA processes.

Compared to PIAs, EIAs are of recent provenance. In 2010/11, different groups of researchers in the USA and in Europe independently proposed principles and procedures for an assessment of the ethical impacts of emerging technologies (Harris et al. 2011; Kenneally et al. 2010; Wright 2011). The goal of an EIA, according to Kenneally et al. (2010), is:

> . . . to further refine these principles into a workable ethical impact assessment (EIA) that can be used as a framework to help ICT researchers think about the ethical impacts of their work.

Although they do not use the exact term 'EIA', Harris et al. (2011) set out:

> . . . a structured meta-methodology for the ethical assessment of new and emerging technologies. It has been designed by a mixture of academics, governmental people and commercial practitioners for the British Computer Society. It is designed to help diverse organisations and individuals conduct ethical assessments of new and emerging technologies.

A point of interest in Harris et al. (2011: 54) is that they specifically include the three perspectives of government, organisation and individual in their meta-methodology. Citing (van den Hoven 2007), they note that:

> Developing, implementing and using technology is never a value-free act.

Like Kenneally et al. (2010) and Wright (2011), their meta-methodology:

> . . . strongly encourages wide consultation, public engagement and debate, which does to some extent identify and challenge underlying assumptions and attitudes. (Harris et al. 2011: 55)

Also like Kenneally et al. (2010) and Wright (2011), they employ questions to help identify and address ethical issues. They advocate a five-step process, known as DIODE (taken from the initial letter of each step):

- Define questions. Ensures that the assessor has defined the technology or project to be examined and is, therefore, able to frame the ethical questions.
- Issues analysis. Ensures that all relevant parties who might be affected are considered (and where appropriate consulted)...
- Options evaluation. Ensures that relevant choices are made...
- Decision determination. Ensures that the assessor can clearly state the ethical decisions made and reasoning behind them... The decision should include guidance on the circumstances which would lead the assessor to revisit the problem.
- Explanations dissemination. Ensures that the decisions are communicated appropriately, including public domain publication wherever possible (Harris et al. 2011: 56–7).

Although the term 'EIA' does not appear before 2009, there have been close analogues to the process, especially in ethical TA. For instance, Skorupinski and Ott (2002: 97) argued that TA, if it is understood as a concept comprising research into the consequences of (intended) technologies and their evaluation, necessarily implies participation in discursive arrangements. They say that TA has several functions, which underscore the relationship between TA and ethics as well as the need to engage stakeholders, including the public, in the assessment process. They say it is not possible without reference to norms and values (Skorupinski and Ott 2002: 98). A policy based merely on expert opinion concerning decisions on technological options suffers from a lack of legitimacy. Thus, an important ethical question is: Who should make a decision about who has to accept which (long-term) consequences (Skorupinski and Ott 2002: 99)? They point out the danger that the decisions for technological developments are taken by a small number of people and many others are then confronted with the consequences (Skorupinski and Ott 2002: 102). They present a comprehensive concept for participatory and discursive TA in 12 'modules' or steps (Skorupinski and Ott 2002: 117–20).

An important contribution in this regard was made by Asveld and Roeser (2009). One section of their book deals with involving the public, and suggests that the inclusion of moral views of the public in risk management is a given.

In a somewhat similar vein, Sollie and Düwel (2011) advanced the methodological ethical assessment of new technologies. In their introductory chapter, they claim that:

> ...although technology is easily one of the most permeating and consequential features of modern society, surprisingly, an ethics of technology is still in its infancy. Important reasons for this 'underdevelopment' of a methodology for morally evaluating technology development are related to its complex, uncertain, dynamic, and large-scale character that seems to resist human control.

On a more political level, in March 2011, President José Manuel Barroso requested the European Group on Ethics in Science and New Technologies (EGE) to draft an Opinion on the ethical issues arising from the rapid expansion of ICT. While the EGE Opinion does not describe an EIA process as such, nevertheless it did emphasise:

> ...the need that when the EU, Member States and relevant stakeholders deliberate, a transparent and participatory model is appropriately incorporated in the decision making process.

They added that:

> This applies to all regulatory initiatives on ICT. (EGE 2012: 63)

The EGE recommended that:

> ...the EU encourages companies to take privacy into consideration when applying their CSR [corporate social responsibility] policy—also using the technological solutions such as PIA, privacy enhancing technology and piracy by design. (EGE 2012: 64)

In summary, it can be said that although the ethics of technology and the assessment of technology impacts both have a long tradition dating back to the 1970s, systematic assessment of the ethical impacts of emergent technologies have only rarely been performed so far. Some ethicists even doubt if such an endeavour can be successful at all (Venier et al. 2013: Chapter 5). We believe, however, that it is necessary and feasible to develop and test such an assessment framework. In this context, it is helpful that EIA is by no means a *sui generis* concept but has many similarities with other, more established impact assessment methodologies.

5. Integrating the two approaches

Perhaps equally inevitable is the notion of integrating PIA, EIA and eventually other impact assessment approaches,[5] for instance, as building blocks in a framework for RRI (von Schomberg 2013: 66). Many advocates of ethical assessment of new technologies already take privacy into account as one of the ethical issues that must be considered in assessing new technologies. Integrating a PIA and an EIA—to develop an integrated P + EIA—is relatively easy to do from a process point of view, but there are challenges as will be outlined in Section 6. Here are the steps that an integrated P + EIA could follow. There may be permutations in the number and sequence of steps depending on the scale of the project under consideration, the numbers of people potentially affected, the needs of the implementing organisation, regulatory requirements etc. For

example, steps 3 and 4 need not be followed sequentially. They could be undertaken concurrently or step 4 could come before step 3. The steps selected are those derived from good practice that we have noted in our reviews of existing PIA methodology and practice. There could be more or fewer steps. They could each be presented in more or less detail. Having made that disclaimer, we think that the steps below provide a useful guide on how PIA and EIA approaches could be integrated.

(1) *Determine whether a PIA or EIA is necessary (threshold analysis):* Generally, if the development and deployment of a new project (or technology or service or policy or other initiative) impacts upon privacy, the project manager should undertake a PIA. The same can be said of a project which raises ethical issues. A P + EIA should be undertaken when it is still possible to influence the design of a project or, if the project is too intrusive upon privacy or raises serious ethical issues or has a negative societal impact, the organisation may need to decide to cancel the project altogether rather than take a decision that is not well supported by stakeholders and suffers from the negative reaction of consumers, citizens, regulatory authorities, the media and/or advocacy groups.

(2) *Identify the P + EIA team and set the team's terms of reference, resources and time frame:* The project manager should be responsible for the conduct of a P + EIA, but may need some additional expertise, perhaps from another organisation. For example, the project manager may decide that an ethicist or someone well-grounded in ethics should be part of the P + EIA team. The project manager and/or the organisation's senior management should decide on the terms of reference for the P + EIA team, its nominal budget and its time frame. The terms of reference should spell out whether public consultations are to be held, to whom the P + EIA report is to be submitted and whether the P + EIA report is to be published. The minimum requirements for a P + EIA will depend on how significant an organisation deems the privacy, ethical or societal risks to be. That an organisation may well downplay the seriousness of the risks makes third-party review and/or audit (see step 13) necessary.

(3) *Prepare a P + EIA plan:* The plan should spell out what is to be done to complete the P + EIA, who on the P + EIA team will do what, the P + EIA schedule and, especially, how the consultation will be carried out. It should specify why it is important to consult stakeholders in this specific instance, who will be consulted and how they will be consulted (e.g. via public opinion survey, workshops, focus groups, public hearings, online). Step 3 can be carried out concurrently with step 4 or in some cases step 4 could be carried out before step 3.

(4) *Describe the proposed project to be assessed:* The description can be used in at least two ways—it can be included in the P + EIA report and it can be used as a briefing paper for consulting stakeholders. The description of the project should provide some contextual information (why the project is being undertaken, who comprises the target market, how it might impact the consumer-citizen's privacy, what personal information will be collected, what ethical issues it might raise, what societal impacts it might have). The project description should state who is responsible for the project. It should indicate important milestones and, especially, when decisions are to be taken that could affect the project's design. A description of the information flows (step 6) could be included as part of the project description.

(5) *Identify stakeholders:* The assessor should identify stakeholders, i.e. those who are or might be interested in or affected by the project, technology or service. The stakeholders could include people who are internal as well as external to the organisation. They could include regulatory authorities, customers, citizen advocacy organisations, suppliers, service providers, manufacturers, system integrators, designers, academics etc. The assessor should identify these different categories and then identify specific individuals from within each of the category, preferably to be as representative as possible. The range and number of stakeholders to be consulted should be a function of the privacy, ethical and societal risks and the assumptions about the frequency and consequences of those risks and the numbers of consumer-citizens who could be impacted.

(6) *Analyse the information flows and other privacy and ethical impacts*: The assessor should consult with others in the organisation and perhaps external to the organisation to describe the information flows and, specifically: who will collect what information from whom for what purpose; how the organisation will use the collected information; how the information will be stored, secured, processed and distributed (i.e. to whom might the organisation pass the information), for what purpose and how well will secondary users (e.g. the organisation's service providers, apps developers) protect that information or will they pass it onto still others? This analysis should be as detailed as possible to help identify potential privacy risks. The assessor should consider the impacts not only on information privacy, but also on other types of privacy (Finn et al. 2013) and, in the instance of an EIA or a societal impact assessment, what ethical issues

the project might raise or what impacts the project might have.

(7) *Consult with stakeholders*: There are many reasons for doing this, not least of which is that they may identify some privacy or ethical or societal risks not considered by the project manager or assessor. By consulting stakeholders, the project manager may forestall or avoid the criticism that they were not consulted. If something does go wrong downstream—when the project or technology or service is deployed—an adequate consultation at an early stage may help the organisation avoid or minimise liability. Furthermore, consulting stakeholders may provide a sort of 'beta test' of the project or service or technology. Stakeholders who have been consulted are less likely to criticise a project than those who have not been consulted.

(8) *Check the project complies with legislation*: A P + EIA is more than a compliance check, nevertheless, either the assessor or their legal experts should ensure that the project complies with any legislative or regulatory requirements or relevant codes of conduct.

(9) *Identify risks and possible solutions*: The assessor and P + EIA team, preferably through stakeholder consultation, should identify possible risks, who those risks will impact and assess those risks for their likelihood (frequency) and consequence (magnitude of impact) as well as the numbers of people who could be affected. Assessing risks, especially ethical ones, is a somewhat subjective exercise. Thus, the assessor will benefit from engaging stakeholder representatives and experts to obtain their views. Deciding how to mitigate or eliminate or avoid or transfer the risk is also a somewhat political decision as is the decision regarding which risks should be retained.

(10) *Formulate recommendations:* The assessor should be clear as to whom the recommendations are directed. Some could be directed towards different units within the organisation, some to the project manager, some to the chief executive officer (CEO), some to employees or employee representatives (e.g. trade unions), to regulatory authorities, third-party apps developers etc. If stakeholders have sight of draft recommendations, before they are finalised, they may be able to suggest improvements to existing recommendations or make additional ones.

(11) *Prepare and publish the report:* Publication of the P + EIA report will increase transparency and trust. Citizen-consumers are more likely to trust an organisation that is open with them than one that provides little or no information about its new technologies or services or other initiatives that affect the citizen-consumer. Some organisations may be afraid to publish their P + EIAs because they fear negative publicity or they have concerns about competitors learning something they do not want them to know. However, where there are legitimate concerns, the organisation can simply redact the sensitive parts or put them into a confidential annex or only provide a summary or, as a last resort, not release the report. However, the report should still be subject to audit in case the true reason for not releasing it was to avoid embarrassment.

(12) *Implement the recommendations:* The project manager and/or the organisation may not accept all of the P + EIA recommendations, but they should say which recommendations they are implementing and why they may not implement others. The organisation's response to the assessor's recommendations should be posted on the organisation's website. This transparency will show that the organisation treats the P + EIA recommendations seriously, which in turn should show consumers and citizens that the organisation merits their trust.

(13) *Third-party review and/or audit of the P + EIA*: Existing PIA reports are of highly variable quality, from the thoughtful and considered to the downright laughable. Some PIA reports exceed 150 pages, others are only a page-and-a-half in length, the sheer brevity of which makes them suspect. Independent, third-party review and/or audits are the only way to ensure P + EIAs are properly carried out and their recommendations implemented. The Office of the Privacy Commissioner of Canada has indicated and extolled the benefits of independent audits (Stoddart 2012). Data protection authorities and/or national ethics committees do not have the resources to audit all P + EIAs, but they could audit a small percentage, enough to make organisations ensure their P + EIAs are reasonably rigorous. Alternatively, independent auditors could undertake this task, just as they audit a company's financial accounts.

(14) *Update the P + EIA if there are changes in the project:* Many projects undergo changes before completion. Depending on the magnitude of the changes, the assessor may need to revisit the P + EIA as if it were a new initiative, including a new consultation with stakeholders.

(15) *Embed privacy and ethical awareness throughout the organisation and ensure accountability:* The CEO is responsible for ensuring that all employees are sensitive to ethical issues and the possible impacts on privacy of what they or their colleagues do. The CEO should be accountable to a supervisory board or shareholders for the adequacy of P + EIA. Embedding an awareness of good ethical practices and of sensitivity to ethical issues also

seems to be worth undertaking by organisations who do not wish to see any harm or damage to their image and reputation.

Fig. 1 illustrates the various steps but, as mentioned at the beginning of Section 4, some steps could be in a different sequence, for instance, step 4 could come before step 3. Elsewhere some steps could take place concurrently or could be iterative. For example, in step 11, the P + EIA team could draft their report and then formulate recommendations and then finalise their report.

The PIA and EIA methodologies we have analysed comprise most of these 15 steps, though some of them are more common than others (Wadhwa and Rodrigues 2013; Wright 2011). Step 2 (Identify the P + EIA team and set the team's terms of reference, resources and time frame) is explicitly mentioned in version 2 of the ICO PIA Handbook. We assume that a similar step is taken in EIAs, especially where a project raises serious ethical issues. Even step 13 (third-party review or independent audit) is common to both PIA and EIA. PIAs may be reviewed by data protection authorities, while EIAs may be subject to review by national ethics committees and/or, for example, university ethics committees. Consequently, the two types of assessment show enough similarity to allow the integration into a single process.

6. Challenges

Despite the relative clarity of the P + EIA process, as described above, an organisation undertaking a P + EIA faces a set of challenges. Some of these challenges are rather generic and can be found in other types of impact assessment. For all that, however, they are amongst the largest challenges to P + EIA, just as they are to other types of assessment.

Finding the right people to undertake the P + EIA is probably the principal challenge. While many P + EIAs can be performed relatively quickly and easily—because the issues they raise are not complicated or the number of people affected is relatively small—others will require a team with a mix of skills (ethicists, privacy experts, information security experts, lawyers, foresight specialists, consultation experts, accountants etc.) some of whom may only be needed for short periods of time. Not all organisations are likely to have all of these competencies. If Article 33 of the proposed Data Protection Regulation is adopted, organisations should try to build their own competencies, but they may need to contract out some tasks.

Identifying and operationalising criteria against which to assess the privacy and ethical impacts may be a challenge and may require inputs from others, perhaps from both internal and external stakeholders. The organisation could undertake this task as part of its overall risk management approach.[6] A particularly difficult task will be the measurement of ethical criteria, though research for the UN has shown that measuring human rights may be feasible (OSHCR 2012). Getting the criteria right is important as it affects the validity and credibility of the assessment.

Regarding the assessment itself, using a sound methodology and engaging some different stakeholders in the process is a challenge. There are few assessment methodologies addressing privacy (and even fewer addressing ethical issues). While there are various PIA methodologies (such as those published by the various regulatory authorities mentioned in Section 3), in fact those methodologies address the process of undertaking a PIA, rather than the actual assessment. While there are various PIA guides and handbooks and even templates for the PIA reports, there are few, almost no, privacy risk assessment methodologies. The closest relevant risk assessment methodologies or standards are those dealing with information security risk management. With few contenders, the CNIL (2012) privacy risk management approach, which is based on EBIOS[7] and ISO 27005 (ISO 2011), stands out as the most relevant one. In fact, it is virtually the only such text to explain in detail how to carry out a privacy risk assessment and what 'controls' an organisation could put in place to manage the privacy risk. In reaction to the upcoming changes of the European privacy legislation, more activities are under way to develop methodologies and techniques to make impact assessments as meaningful and easy to conduct as possible.[8]

Identifying the privacy and ethical risks is also challenging. Identifying risks should be done systematically, taking future threats and vulnerabilities into account. Again, the collaboration of stakeholders will be helpful in this regard.

Considering the privacy and ethical impacts of new and emerging technologies is a difficult challenge, because technologies may have intended as well as unintended consequences. Beyond the purpose for which they are being developed, new technologies may lead to function creep and be used in ways that are not yet immediately apparent.

Finding and encouraging stakeholders to participate in consultation exercises is a challenge. The phenomenon of 'consultation fatigue' is well known (Riege and Lindsay 2006: 35). For the project manager or P + EIA assessor, it is important to have a range of stakeholders represented in the process, so that one particular group (e.g. industry with much deeper pockets than advocacy groups) does not dominate the process. The assessor needs to identify the range of stakeholders who are interested in, or potentially affected by, a new technology and then pro-actively encourage representatives from each group of stakeholders to participate in the process. There is a range of consultation techniques which can be used, such as: Delphi surveys, focus groups, online consultations, interviews and citizen panels (Slocum et al. 2006).

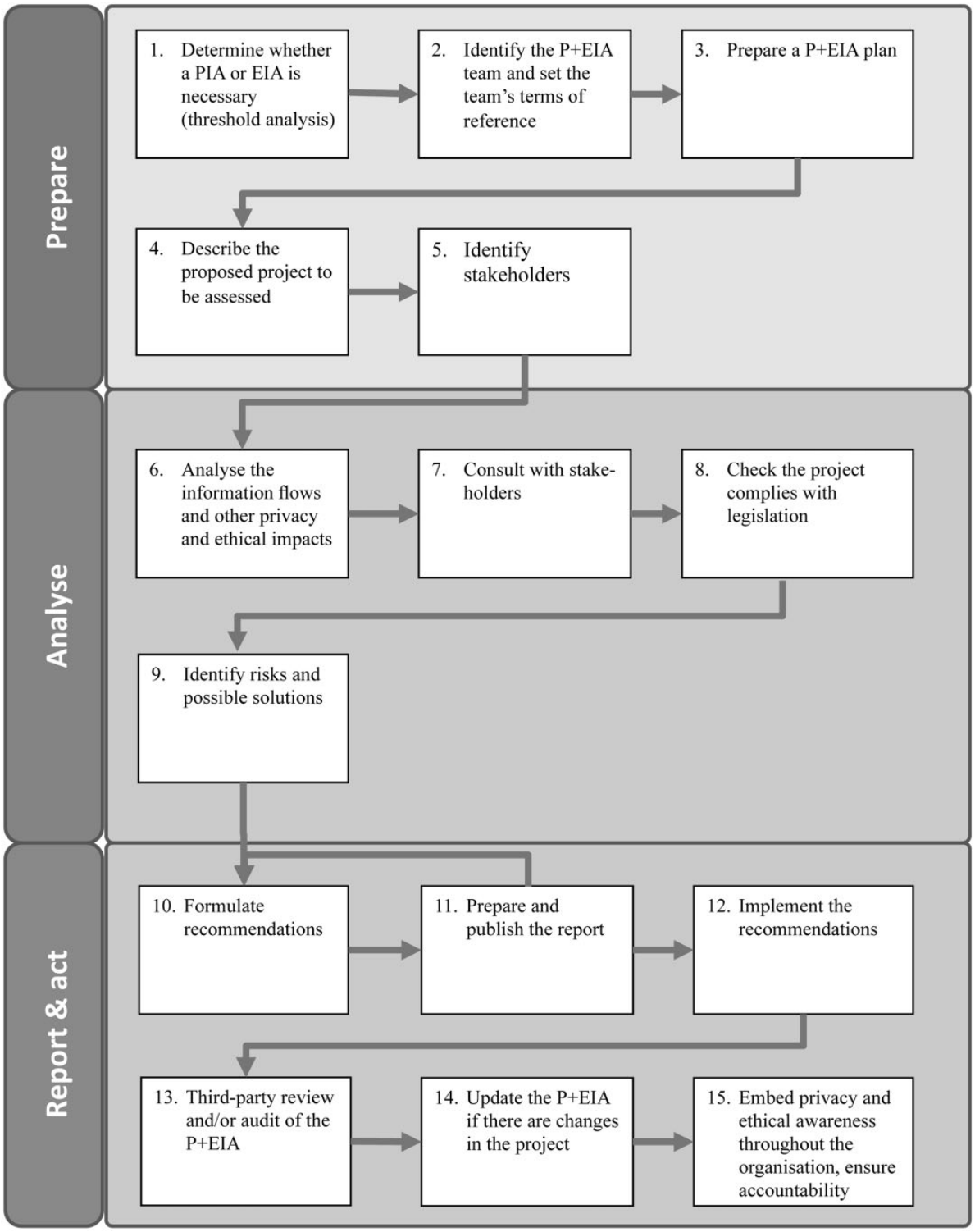

Figure 1. Steps in the P + EIA process.

Two other challenges—the most contentious steps in the process—are publication of the PIA and/or EIA reports and making them subject to third-party review or audit. Some PIA reports are now published. For instance, US government agencies now have online repositories of their PIA reports. Private sector organisations are especially reluctant to publish their PIA reports. Indeed, the very mention of the idea makes some entrepreneurs apoplectic. Still, few would dispute that publication of PIA reports (even redacted ones) helps to improve trust and transparency. Properly carried out, the publication of the report, like that of consultation with stakeholders, may

result in the generation of new ideas of value to the project manager.

A key policy issue now, is that Article 33 of the proposed Regulation is of somewhat limited scope and does not always apply. It focuses only on data protection (information privacy) and not on all types of privacy or ethical issues. However, the proposed Regulation is still under consideration in the European Parliament and Council (as of summer 2013) and it may still be modified before it is adopted. The outcome of Article 33 is difficult to guess at this stage.

7. Conclusions

Despite the challenges, we believe it is useful and desirable to develop an integrated P + EIA, not only because Data Protection Impact Assessment (DPIA) is becoming mandatory for certain technologies according to the proposed Data Protection Regulation. In particular, the process for conducting a PIA and an EIA can be more or less the same. As many experts have noted, some new technologies raise privacy and ethical issues, such as: human dignity, equality, non-discrimination or self-determination. Thus, those issues should be addressed before a new technology is deployed. Developers, whether from government or industry, who choose to ignore public opinion or the views of stakeholders risk a backlash from voters or shareholders as well as damage to their reputation and undermining the trust of citizen-consumers.

In the last few years, the EC has been urging researchers to consider data protection, ethical and social impact issues in the context of its Framework Programme for Research and Innovation. The EC's interest in such issues is unlikely to diminish. On the contrary, it will become an inherent part of European research policy. Having a comprehensive framework within which to do this assessment would certainly improve the quality of research in regard to these issues.

Perhaps the most important reason for undertaking a P + EIA is that it will improve transparency, which is needed to build trust with citizen-consumers.

Funding

This work was supported by the European Commission's Seventh Framework Programme for Research and Innovation (PRESCIENT project under grant agreement number 244779; PIAF project under grant agreement number JUST/2010/FRAC/AG/1137-30-CE-0377117/00-70).

Notes

1. Solove (2008: 12) describes privacy as:

   > . . . a concept in disarray. Nobody can articulate what it means.

2. This close relationship of the modern privacy concept was already been addressed in the first seminal publication by Warren and Brandeis (1890). They defined privacy as response to (then) new technological developments in photography (George Eastman had introduced the first film in roll form in 1884 and the 'snap camera' in 1888) and the new practices based upon them (photo journalism and yellow press).
3. More detailed information on these countries and a comparison of different PIA methodologies can be found in Wright et al. (2011) and Wright and De Hert (2012), respectively.
4. The Privacy Commissioner acknowledges (OVPC 2009: xviii) that there may be circumstances where the full or part release of a PIA may not be appropriate. For example, the project may still be in its very early stages. There may also be security, commercial-in-confidence or, for private sector organisations, other competitive reasons for not making a PIA public in full or in part. However, transparency and accountability are key issues for good privacy practice and outcomes, so where there are difficulties making the full PIA available, the Privacy Commissioner encourages organisations to consider the release of a summary version.
5. See, for instance, the EST-Frame project, which aims to develop appropriate tools for social impact assessment and technology evaluation <http://estframe.net/> accessed 08 November 2013.
6. The ISO 27005 standard on Information Security Risk Management is one of the most widely used and can be adapted relatively easily to focus on privacy risk assessment and management.
7. EBIOS = Expression des besoins et identification des objectifs de sécurité <http://www.ssi.gouv.fr/en/the-anssi/publications-109/methods-to-achieve-iss/ebios-2010-expression-of-needs-and-identification-of-security-objectives.html> accessed 08 November 2013.
8. For instance, the UK Information Commissioner's Office has revised its PIA handbook; the EC Seventh Framework Programme for Research and Innovation projects SAPIENT (<http://www.sapientproject.eu> accessed 08 November 2013) and SIAM (<http://www.siam-project.eu> accessed 08 November 2013) are developing guidelines to assess the privacy and ethical impacts of surveillance and other security technologies.

References

Asveld, L. and Roeser, S. (2009) *The Ethics of Technological Risk*. London: Earthscan.

Böhle, K., Coenen, C., Decker, M. and Rader, M. (2013) 'Biocybernetic adaptation and privacy', *Innovation: The European Journal of Social Science Research*, 26: 71–80.

Cabinet Office. (2008a) 'Data Handling Procedures in Government: Final Report'. London: Cabinet Office, <http://www.cabinetoffice.gov.uk/sites/default/files/resources/final-report.pdf> accessed XX XXXXXXX XXXX.

————. (2008b) 'Cross Government Actions: Mandatory Minimum Measures'. London: Cabinet Office, <http://www.cabinetoffice.gov.uk/sites/default/files/resources/cross-gov-actions.pdf> accessed 08 November 2013.

Clarke, R. (2009) 'Privacy impact assessment: Its origins and development', *Computer Law & Security Review*, 25: 123–35.

—— (2012) 'PIAs in Australia: A Work-in-Progress Report'. In: Wright, D. and De Hert, P. (eds) *Privacy Impact Assessment*, pp. 119–48. Berlin: Springer.

CNIL (Commission Nationale de l'Informatique et des Libertés). (2012) 'Methodology for Privacy Risk Assessment: How to implement the Data Protection Act'. Paris: CNIL, <http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Methodology.pdf> accessed 08 November 2013.

EC (European Commission). (2012) 'Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)', COM(2012) 11 final. Brussels: European Commission.

EGE (European Group on Ethics in Science and New Technologies to the European Commission). (2012) 'Ethics of Information and Communication Technologies', Opinion No. 26. Luxembourg: Publications Office of the European Union.

Finn, R. L., Wright, D. and Friedewald, M. (2013) 'Seven types of privacy'. In: Gutwith, S. *et al*. (eds) *European Data Protection: Coming of Age*, pp. 3–32. Berlin: Springer.

——, Friedewald, M., Gellert, R., Gutwirth, S. *et al*. (2011) 'Privacy, data protection and ethical issues in new and emerging technologies: Five case studies'. PRESCIENT Project, Deliverable 2 <http://prescient-project.eu/prescient/inhalte/download/PRESCIENT_D2.pdf> accessed 08 November 2013.

Gutwirth, S., Gellert, R., Bellanova, R., Friedewald, M. *et al*. (2011) 'Legal, social, economic and ethical conceptualisations of privacy and data protection'. PRESCIENT Project, Deliverable 1 <http://prescient-project.eu/prescient/inhalte/download/PRESCIENT-D1—final.pdf> accessed 08 November 2013.

Hallinan, D., Schütz, P., Friedewald, M., De Hert, P. *et al*. (2014) 'Neurodata and data protection: Should we be mindful of data of the mind?', *Surveillance and Society*, 12: Forthcoming.

Harris, I., Jennings, R. C., Pullinger, D., Rogerson, S. and Duquenoy, P. (2011) 'Assessment of new technologies: A meta-methodology', *Journal of Information, Communication and Ethics in Society*, 9: 49–64.

HIQA (Health Information and Quality Authority). (2010a) 'International Review of Privacy Impact Assessments'. Cork, Ireland: HIQA, <http://www.hiqa.ie/publications/international-review-privacy-impact-assessments> accessed 08 November 2013.

————. (2010b) 'Guidance on Privacy Impact Assessment in Health and Social Care'. Dublin: HIQA, <http://www.hiqa.ie/system/files/HI_Privacy_Impact_Assessment.pdf> accessed XX XXXXXXX XXXX.

ICO (Information Commissioner's Office). (2009) 'Privacy Impact Assessment Handbook. Version 2.0'. Wilmslow, UK: UK Information Commissioner's Office, <http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/index.html> accessed 08 November 2013.

ISO (International Organization for Standardization). (2011) 'Information Technology - Security Techniques - Information Security Risk Management' ISO/IEC 27005:2011. Geneva: International Organization for Standardization.

Kenneally, E., Bailey, M. and Maughan, D. (2010) 'A framework for understanding and applying ethical principles in network and security research', in *Financial Cryptography and Data Security. FC 2010 Workshops, RLCPS, WECSR, and WLC 2010, Tenerife, Canary Islands, Spain, January 25–8, 2010, Revised Selected Papers* (Lecture Notes in Computer Science 6054), R. Sion, R. Curtmola, S. Dietrich and A. Kiayias (eds), pp. 240–46. Berlin: Springer.

OAIC (Office of the Australian Information Commissioner). (2010) 'Privacy Impact Assessment Guide'. Sydney: OAIC, <http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/privacy-impact-assessment-guide> accessed 08 November 2013.

OIPC (Office of the Information and Privacy Commissioner of Alberta). (2009) 'Privacy Impact Assessment Requirements', Edmonton, Canada: OIPC, <http://www.oipc.ab.ca/Content_Files/Files/PIAs/PIA_Requirements_2010.pdf> accessed 08 November 2013.

OMB (Office of Management and Budget). (2003) 'OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002', Washington, DC, <http://www.whitehouse.gov/omb/memoranda/m03-22.html> accessed 08 November 2013.

OPC (Office of the Privacy Commissioner). (2007) 'Privacy Impact Assessment Handbook', Wellington, New Zealand, <http://privacy.org.nz/assets/Files/Brochures-and-pamphlets-and-pubs/48638065.pdf> accessed 08 November 2013.

OSHCR (Office of the UN High Commissioner for Human Rights). (2012) 'Human Rights Indicators: A Guide to Measurement and Implemetation', HR/PUB/12/5. UN: New York.

OVPC (Office of the Victorian Privacy Commissioner). (2009) 'Privacy Impact Assessments: A guide for the Victorian Public Sector (Edition 2). Melbourne, Australia: OVPC.

Owen, R., Macnaghten, P. and Stilgoe, J. (2012) 'Responsible research and innovation: From science in society to science for society, with society', *Science and Public Policy*, 39: 751–60.

Ozoliņa, Z., Mitcham, C., ——, Andana, P. *et al*. (2012) 'Ethical and Regulatory Challenges to Science and Research Policy at the Global Level'. Luxembourg: Publications Office of the European Union.

——, ——, Schroeder, D., Mordini, E. *et al*. (2009) 'Global Governance of Science', Report of the Expert Group on Global Governance of Science to the Science, Economy and Society Directorate, Directorate-General for Research, European Commission. Luxembourg: Office for Official Publications of the European Communities.

Riege, A. and Lindsay, N. (2006) 'Knowledge management in the public sector: Stakeholder partnerships in the public policy development', *Journal of Knowledge Management*, 10(3): 24–39.

Skorupinski, B. and Ott, K. (2002) 'Technology assessment and ethics', *Poiesis and Praxis*, 1: 95–122.

Slocum, N., Steyaert, S. and Berloznik, R. (2006) *Participatory Methods Toolkit: A Practitioner's Manual*. Brussels: King Baudouin Foundation.

Sollie, P. and Düwel, M. (2011) *Evaluating New Technologies: Methodological Problems for the Ethical Assessment of Technology Developments*. Berlin: Springer.

Solove, D. J. (2008) *Understanding Privacy*. Cambridge, MA: Harvard University Press.

Spiekermann, S. (2012) 'The RFID PIA: Developed by industry, endorsed by regulators'. In: Wright, D. and De Hert, P. (eds) *Privacy Impact Assessment*, pp. 323–46. Berlin: Springer.

Stahl, B. C. (2013) 'Responsible research and innovation: The role of privacy and ethics in an emerging framework', *Science and Public Policy*, 40: XXX–XXX, (this issue).

Stoddart, J. (2012) 'Auditing privacy impact assessments: The Canadian experience'. In: Wright, D. and De Hert, P. (eds) *Privacy Impact Assessment*, pp. 419–36. Berlin: Springer.

Taylor, M. (2012) *Genetic Data and the Law: A Critical Perspective on Privacy Protection*. Cambridge, UK: CUP.

TBS (Treasury Board of Canada Secretariat). (2002) 'Privacy Impact Assessment Guidelines: A Framework to Manage Privacy Risks'. Ottawa: TBS, <http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paipg-pefrld1-eng.asp> accessed 08 November 2013.

————. (2010) 'Directive on Privacy Impact Assessment'. Ottawa: TBS.

van den Hoven, J. (2007) 'ICT and value sensitive design'. In: Goujon, P., Lavelle, S., Duquenoy, P., Kimppa, K. and Laurent, V. (eds) *The Information Society: Innovation, Legitimacy, Ethics and Democracy*, pp. 67–72. Berlin: Springer.

Venier, S. and Mordini, E. (eds) (2013) 'Final Report – A Privacy and Ethical Impact Assessment Framework for Emerging Sciences and Technologies', PRESCIENT Project, Deliverable 4 <http://prescient-project.eu/prescient/inhalte/download/PRESCIENT_deliverable_4_final.pdf> accessed 08 November 2013.

von Schomberg, R. (2011) 'Prospects for technology assessment in a framework of responsible research and innovation'. In: Dusseldorp, M. and Beecroft, R. (eds) *Technikfolgen abschätzen lehren. Bildungspotenziale transdisziplinärer Methoden*, pp. 39–61. Berlin: Springer.

—— (2013) 'A vision of responsible research and innovation'. In: Owen, R., Bessant, J. and Heintz, M. (eds) *Responsible Innovation*, pp. 51–74. Chichester, UK: Wiley.

Wadhwa, K. and Rodrigues, R. (2013) 'Evaluating privacy impact assessments', *Innovation: The European Journal of Social Science Research*, 26: 161–80.

Warren, S. D. and Brandeis, L. D. (1890) 'The Right To Privacy', *Harvard Law Review*, 4/5: 193–220.

Wright, D. (2011) 'A framework for the ethical impact assessment of information technology', *Ethics and Information Technology*, 13: 199–226.

—— (2012) 'The state of the art in privacy impact assessment', *Computer Law & Security Review*, 28: 54–61.

—— and De Hert, P. (2012) 'Introduction to privacy impact assessment'. In: Wright, D. and De Hert, P. (eds) *Privacy Impact Assessment*, pp. 3–32. Berlin: Springer.

——, Wadhwa, K., De Hert, P. and Kloza, D. (2011) 'A privacy impact assessment framework for data protection and privacy rights (PIAF Deliverable 1)'. London and Brussels: Trilateral Research and Consulting and Vrije Universiteit Brussels, <www.piafproject.eu/ref/PIAF_D1_21_Sept2011Revlogo.pdf> accessed 08 November 2013.