Integrating privacy and ethical impact assessments

David Wright
Michael Friedewald, Fraunhofer Institute for Systems and Innovation Research

Available at: https://works.bepress.com/michael_friedewald/66/
Integrating privacy and ethical impact assessment

David Wright and Michael Friedewald

New and emerging technologies often raise ethical as well as privacy issues. The analysis and assessment of such issues is the task of privacy impact assessments (PIAs) and ethical impact assessments (EIAs). 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.

In this paper, we briefly review PIAs and EIAs and propose an integration of the two methodologies in line with the notion of ‘responsible research and innovation’ (RRI). For this purpose we are, in section 2, outlining 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 different countries and the European Union. In section 4 we argue that PIAs and EIAs could follow similar processes, which lend themselves to their integration, such integration nevertheless faces certain challenges which are outlined here. The paper concludes that there are several reasons why such an integration is not only feasible, but useful and merits the attention of policy-makers and project managers alike.

1 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’ (Ozoliņa et al. 2009: p. 7) 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 in the scope of policy-makers but already recognised as future challenges. Since then, privacy has become an important topic in the work done or funded by the European Commission. Many experts have commented on the difficulty of defining privacy. Daniel 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: p. ix) Not everyone sees the lack of an agreed definition as a problem. Finn et al. (2013: p. 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 European Union. It is often regarded as an ethical issue as well, as reflected in a recent report of the European Group on Ethics in

---

1 Solove describes privacy as “a concept in disarray. Nobody can articulate what it means” (Solove 2008: p. 12).
Science and New Technologies (EGE 2012). The PRESCIENT consortium, of which the authors of this paper were partners, commented on privacy and ethics thusly:

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: p. 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 them by creating the possibility to create and to 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 into account this rich and nuanced interplay between technology and privacy 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 research and development on 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, among others (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 policymakers and decision-takers to better balance countervailing interests.

² This close relationship of modern privacy concept has 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, yellow press).
Since 2009, the EC has also promoted the concept of ‘responsible research and innovation’ (RRI) which has gained increasing EU policy relevance (Owen et al. 2012; Stahl 2013). According to von Schomberg (2011: p. 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 (Ozoliņa 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 privacy impact assessments (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 European Commission (DG INFSO, now DG Connect) initiated the development of a PIA framework for RFID applications (Spiekermann 2012), at the same time DG Justice explored national PIA schemes and good practice elements (Wadhwa and Rodrigues 2013). Finally the Commission 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 (European Commission 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 article proposes how to integrate privacy and ethical impact assessments as an element of the future framework for the governance of emerging technologies.

2 PRIVACY IMPACT ASSESSMENT

Privacy impact assessment 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: p. 55). Privacy impact assessment 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 US. While there are differences in the methodologies, all of them are concerned with identifying risks to privacy and ways of overcoming those risks. The following paragraphs offer a thumbnail sketch of the principal PIA policies and methodologies.

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

---

3 Radio Frequency Identification
4 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.
(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 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.\(^5\)

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 Victorian public sector, 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).

**Canada**

In Canada, the Treasury Board Secretariat (TBS) issued PIA Guidelines in August 2002 (TBS 2002). It promulgated a new Directive on Privacy Impact Assessment in April 2010 (TBS 2010). The directive ties PIAs with submissions to the Treasury Board for program 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.

**Ireland**

The Health Information and Quality Authority 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 Health Information and Quality Authority favours 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.

\(^5\) The Privacy Commissioner acknowledges (OVPC 2009: p. 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 Commissioner encourages organisations to consider the release of a summary version.
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.

United Kingdom

The Information Commissioner’s Office (ICO) in the United Kingdom 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). 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 in its Handbook.

United States

In the United States, privacy impact assessments 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).

European Union

Article 33 of the European Commission’s proposed new Data Protection Regulation would make data protection impact assessments (otherwise known as privacy impact assessments, 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 European Union – and beyond too, especially where non-EU organisations which to sell products or provide services in Europe. Finally the Regulation could serve as a template for 3rd state regulation; consequently the PIA scheme that it will finally adopt could give momentum to the development towards 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 to demonstrate compliance with the Regulation. Interestingly,
the proposed Regulation would require data controllers to seek the views of data subjects or their representatives on the intended processing.

The PIA requirements described in Article 33 are rather sketchy, hence, the Commission includes a provision that would empower it to specify additional criteria and conditions at a later time, including conditions for ‘scalability, verification and auditability’. It would also be empowered to specify standards and procedures for carrying out, verifying and auditing PIAs. There is, however, high criticism that the detailed requirements on whether a specific data processing is considered as risky and how in this the PIA has to be carried out will be defined by way of delegated or implementing acts through the European Commission (e.g. Art 29 WP2012; Hornung 2012).

3 ETHICAL IMPACT ASSESSMENT

Much can be (and has been) learned from a review of these different methodologies in designing a more optimised approach to P+EIA, as discussed further below. 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 we can see a distinct evolution in enhancing PIA processes.

Compared to privacy impact assessments, ethical impact assessments (EIAs) are of recent provenance. In 2010/11, different groups of researchers in the US and in Europe independently proposed principles and procedures for an assessment of 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 ‘ethical impact assessment’, 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: p. 54). is that they specifically include the three perspectives or 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 the two preceding papers, 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: p. 55). Also like the two previously cited papers, they employ questions to help identify and address ethical issues. They advocate a five-step process called DIODE (taken from the initial letter of each step):

(1) Define questions. Ensures that the assessor has defined the technology or project to be examined and is, therefore, able to frame the ethical questions.
(2) Issues analysis. Ensures that all relevant parties who might be affected are considered (and where appropriate consulted)...
(3) Options evaluation. Ensures that relevant choices are made...
(4) 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.

(5) Explanations dissemination. Ensures that the decisions are communicated appropriately, including public domain publication wherever possible (Harris et al. 2011: p. 56-7).

Although the term ‘ethical impact assessment’ does not appear before 2009, there have been close analogues to the process, especially in ethical technology assessment. For instance, Skorupinski and Ott (2002: p. 97) argued that technology assessment, 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 technology assessment has several functions, which underscores 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 (p. 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 (p. 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 (p. 102). They present a comprehensive concept for participatory and discursive TA in 12 ‘modules’ or steps (p. 117-20).

An important contribution in this regard was Asveld and Roesser’s (2009) collection, The Ethics of Technological Risk. One section of the book deals with involving the public, and suggests that the inclusion of moral views of the public in risk management is a given.

In somewhat the same vein was the book edited by Sollie and Düwel (2011) who advanced the methodological ethical assessment of new technologies. In their introductory chapter, they claim that “[a]lthough 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 Information and Communication Technologies. While the EGE Opinion does not describe an ethical impact assessment 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: p. 63). The EGE added that it recommended that ‘the EU encourages companies to take privacy into consideration when applying their CSR policy – also using the technological solutions such as Privacy impact assessment, Privacy enhancing technology and piracy by design’ (EGE 2012: p. 64).

In summary it can be said, therefore, that though the ethics of technology and the assessment of technology impacts both have a long tradition dating back until the 1970s, systematic assessment of ethical impacts of emergent technologies have been performed rarely yet. 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 ethical impact assessment is by no
means a *sui generis* concept but has many similarities with other, more established impact assessment methodologies.

## 4 INTEGRATING THE TWO APPROACHES

Perhaps equally inevitable is the notion of integrating PIA, EIA and eventually other impact assessment approaches⁶, e.g., as building blocks in a framework for responsible research and innovation (e.g., von Schomberg 2013: p. 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, as follows, but there are challenges as outlined in the next section. 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 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 suffer from the negative reaction of consumers, citizens, regulatory authorities, the media and/or advocacy gadflies.

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 she may need some additional expertise, perhaps from outside her 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, the budget for the assessment, the time frame, 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

---

⁶ See, for instance, the EST-Frame project, which aims to develop appropriate tools for social impact assessment and technology evaluation. http://estframe.net/
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 and so on. 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 will the organisation use the collected information; how will the information be stored, secured, processed and distributed (i.e., to whom might the organisation pass on 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 on to 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 other types of privacy as well (Finn et al. 2013) and, in the instance of ethical impact assessment or 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 so, 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 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. Consulted stakeholders are less likely to criticise a project than those who were not consulted.
8. **Check the project complies with legislation:** A privacy and ethical impact assessment is more than a compliance check, nevertheless, the assessor or her 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 her 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 have 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 to retain.

10. **Formulate recommendations:** The assessor should be clear to whom her recommendations are directed – some could be directed towards different units within the organisation, some to the project manager, some to the 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 on 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 don’t want them to. However, where there are legitimate concerns, the organisation can simply redact the sensitive bits or put them into a confidential annex or provide only 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 chief executive officer 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 her 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.

The diagram below illustrates the various steps, but as mentioned at the outset of section 4, some steps could be in a different sequence, e.g., 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.

5 **CHALLENGES**

Despite the relative clarity of the P+EIA process, as described above, the 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 among the biggest 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 and so on – some of whom may be needed only 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.\(^7\) A particularly difficult task will be the measurement of ethical criteria, though research for the United Nations 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, ethical issues). While there are various PIA methodologies (such as those published by the various regulatory authorities mentioned above 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\(^8\) and ISO 27005 (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.\(^9\)

Identifying the privacy and ethical risks is a challenge too. Identifying risks should be done systematically, taking into account future threats and vulnerabilities. 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 (e.g. Riege and Lindsay 2006: p. 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 are a range of consultation techniques which can be used,

---

\(^7\) 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.


\(^9\) For instance, the UK Information Commissioner’s Office has revised its PIA handbook; the FP7 projects SAPIENT (http://www.sapientproject.eu) and SIAM (http://www.siam-project.eu) are developing guidelines to assess privacy and ethical impacts of surveillance and other security technologies.
e.g., Delphi surveys, focus groups, online consultations, interviews, citizen panels, etc. (Slocum et al. 2006).

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 published now, e.g., US government agencies 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. Even after its adoption, the Commission might decide to expand the scope of Article 33 in a delegated implementing act, but the outcome of Article 33 is difficult to guess at this stage.

6 CONCLUSIONS

Despite the challenges, we believe it is useful and desirable to develop an integrated P+EIA – not only because DPIA is becoming mandatory for certain technologies according to the proposed data protection regulation. In particular, the process for conducting a privacy impact assessment and an ethical impact assessment 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. Hence, those issues should be addressed before a new technology is deployed. A developer, whether from government or industry, who chooses to ignore public opinion or the views of stakeholders risks facing a backlash from voters or shareholders as well as damage to his reputation and undermining the trust of citizen-consumers.

In the last few years, the European Commission is urging researchers to consider data protection, ethical and social impact issues in the context of its Framework research programmes. The Commission’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 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+EAI 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 7th Framework Programme for Research and Innovation [PRESIENT project under grant agreement number 244779; PIAF project under grant agreement number JUST/2010/FRAC/AG/1137-30-CE-0377117/00-70].
REFERENCES


