

# Privacy by design



## Foreword

The capacity of organisations to acquire and use our personal details has increased dramatically since our data protection laws were first passed. There is an ever-increasing amount of personal information collected and held about us as we go about our daily lives. Although we have seen a dramatic change in the capability of organisations to exploit modern technology that uses our information to deliver services, this has not been accompanied by a similar drive to develop new effective technical and procedural privacy safeguards. We have seen how vulnerable our most personal of details can be and these should not be put at risk. The Information Commissioner's Office (ICO) commissioned this expert report to try to identify why more has not been done to design in privacy protections from first principles and what needs to be done to rectify the situation. This report provides a thorough analysis of the situation and we will be considering what action we can take based upon its helpful recommendations with the aim of achieving a comprehensive approach to securing privacy protection.

**Richard Thomas, Information Commissioner**  
**26th November 2008**

The privacy by design programme will encourage public authorities and private organisations to ensure that as information systems that hold personal information and accompanying procedures are developed, privacy concerns are identified and addressed from first principles. In short, this means designing in privacy and data protection compliance rather than ignoring it or bolting it on as an inadequate afterthought.

Over recent months the Enterprise Privacy Group has consulted with a cross-section of privacy, identity and security experts, hosted an expert workshop and drawn upon past and ongoing research into privacy-related topics to build up a view of the actions that could reinvigorate respect for privacy needs in the systems lifecycle. This has resulted in a wealth of materials and original work, and these will be published to support this document.

This report is the first stage in bridging the current gap in the development and adoption of privacy-friendly solutions as part of modern information systems. It aims to address the current problems related to the handling of personal information and put into place a model for privacy by design that will ensure privacy achieves the same structured and professional recognition as information security has today.

Our publication is only the first step in a journey towards privacy by design. The project will develop from this point, exploring the key issues in greater detail, refining recommendations and putting them into practice.

We wish to extend our appreciation to everyone who has contributed to this report.

**Toby Stevens, Director, Enterprise Privacy Group**  
**26th November 2008**

# Privacy by design – Executive summary

Over the past year a stream of high-profile data loss incidents have shaken consumer confidence in the ability of public authorities and private organisations to manage personal information in a trustworthy manner. There is a clear and urgent need for a new approach that will help to reduce the risks arising from processing personal information and hence rebuild consumer trust. This is the purpose of **Privacy by Design**.

The privacy by design approach that is described in this report will encourage organisations to give due consideration to privacy needs prior to the development of any new system or process, and to maintain that control throughout the systems lifecycle, from the earliest stages of developing a business case, through to the decommissioning of the system. This lifetime approach will ensure that privacy controls are stronger, simpler to implement, harder to by-pass, and totally embedded in the system's core functionality.

A 'privacy by design ecosystem' is required – an environment in which organisations understand what is expected of them and how to deliver it, supported by innovative delivery of privacy enhancing technologies (PETs) from vendors, and an ICO that can both support and enforce fresh standards for the handling of personal information.

However, if privacy by design is to be successful then a number of important barriers to its adoption must be removed. At present there is an ongoing lack of awareness of privacy needs at an executive management level, driven by uncertainty about the potential commercial benefits of privacy-friendly practices; a lack of planning for privacy functionality within the systems lifecycle; fundamental conflicts between privacy needs and the pressure to share personal information within and outside organisations; few delivery standards with which organisations can comply; a need for off-the-shelf PETs to simplify delivery of privacy functionality; and a role for an empowered and properly-resourced ICO to ensure that organisations step up to the mark in their handling of personal information.

To remove these barriers, and stimulate the development of privacy by design, the Enterprise Privacy Group has developed a number of recommendations for government, regulators, industry, academia and privacy practitioners to pursue, with the support and encouragement of the ICO. These recommendations include the following:

- Working with industry bodies to build an **executive mandate for privacy by design**, supported by sample business cases for the costs, benefits and risks associated with the processing of personal information, and promotion of executive awareness of key privacy and identity concepts so that privacy is reflected in the business cases for new systems.
- Encouraging widespread use of **privacy impact assessments throughout the systems lifecycle**, and ensuring that these assessments are both maintained and published where appropriate to demonstrate transparency of privacy controls.
- Supporting the development of **cross-sector standards for data sharing** both within and between organisations, so that privacy needs are harmonised with the pressures on public authorities and private organisations to share personal information.
- Nurturing the development of **practical privacy standards** that will help organisations to turn the legal outcomes mandated under data protection laws into consistent, provable privacy implementations.
- **Promoting current and future research into PETs** that deliver commercial products to manage consent and revocation, privacy-friendly identification and authentication, and prove the effectiveness of privacy controls.
- **Establishing more rigorous compliance and enforcement mechanisms** by assigning responsibility for privacy management within organisations to nominated individuals, urging organisations to demonstrate greater clarity in their personal information processing, and empowering and providing the ICO with the ability to investigate and enforce compliance where required.

The government, key industry representatives and academics, and the ICO are urged to consider, prioritise and set in motion plans to deliver these recommendations and hence make privacy by design a reality.

## Privacy by design: Summary of barriers, desired outcomes and recommendations

Theme	Barriers to privacy by design	Desired privacy outcomes	Recommendations for delivering privacy by design
<b>Engaging executive management</b>	<ul style="list-style-type: none"> <li>■ Executive managers don't always recognise or correctly prioritise their organisation's responsibility or their own accountability for protecting individuals' privacy.</li> <li>■ Executives and their staff often lack a shared language to discuss or to specify privacy requirements in a clear unambiguous way. As a result, poor privacy specifications deliver poor privacy controls.</li> <li>■ Commercial risks and benefits of managing personal information are often unclear, making it hard to justify privacy investment. In consequence privacy needs are often omitted from the business cases for new systems.</li> </ul>	<ul style="list-style-type: none"> <li>■ Executive managers understand their privacy duties and communicate their privacy management wishes across the organisation.</li> <li>■ Business cases for new systems incorporate privacy specifications that are understood by all members of staff.</li> </ul>	<ul style="list-style-type: none"> <li>■ The executive managers of public authorities and private organisations need greater awareness of their privacy responsibilities, and this should be supported by:                             <ul style="list-style-type: none"> <li>- providing sample costs, risks and benefits cases to demonstrate the value of privacy compliance; and</li> <li>- promoting a simple shared language for key privacy concepts such as data minimisation, identification, authentication and anonymisation to assist communication within and outside of organisations.</li> </ul> </li> </ul> <p>The ICO and other regulatory bodies have a role in making this happen.</p>
<b>Planning for privacy by design</b>	<ul style="list-style-type: none"> <li>■ Traditional risk management methodologies often fail to consider the value of personal information, and hence do not take privacy needs into account.</li> <li>■ Risk assessment approaches often fail to manage privacy needs throughout the systems lifecycle, so many bespoke and off-the-shelf systems are still built without proper or innovative privacy controls.</li> <li>■ Privacy needs are often not rigorously considered at any stage of the systems lifecycle, so systems can be modified or re-used without consideration for privacy implications.</li> <li>■ Systems do not always support automated subject access requests, and hence information retrieval procedures can be onerous for organisations.</li> </ul>	<ul style="list-style-type: none"> <li>■ Systems incorporate appropriate PETs based upon a rigorous privacy impact assessment.</li> <li>■ Privacy needs are managed throughout the systems lifecycle.</li> </ul>	<ul style="list-style-type: none"> <li>■ Organisations should be encouraged to implement high-level privacy management policies that will call for:                             <ul style="list-style-type: none"> <li>- incorporating privacy impact assessments throughout the systems lifecycle from business case to decommissioning;</li> <li>- managing privacy-related risks to within pre-defined levels;</li> <li>- potentially submitting privacy impact assessments for the most sensitive systems to the ICO for verification; and</li> <li>- promoting greater transparency by publishing privacy impact assessments (this possibly being mandatory for public sector organisations).</li> </ul> </li> <li>■ Organisations should be urged to demonstrate that all new systems support automated subject access requests, and encouraged to implement online subject access request services where appropriate.</li> </ul>
<b>Sharing personal information</b>	<ul style="list-style-type: none"> <li>■ The pressure to share personal information within and outside of organisations can lead to privacy-related problems:                             <ul style="list-style-type: none"> <li>- data from 'privacy-friendly' systems is shared with other systems that are less able to respect privacy needs;</li> <li>- copies of personal information in transit are not always appropriately secured;</li> <li>- organisations often aggregate data rather than sharing it;</li> <li>- identifiers are used as indices, making it hard to anonymise data thereafter; and</li> <li>- privacy metadata can be lost as information is shared between systems.</li> </ul> </li> <li>■ If system PIAs are conducted in isolation the results may fail to take into account the broader systemic implications of data sharing.</li> </ul>	<ul style="list-style-type: none"> <li>■ Organisations can share data internally and externally, and individuals have confidence that their privacy wishes will be respected when they do so.</li> <li>■ Individuals know who has their personal information and are able easily to access and amend it.</li> </ul>	<ul style="list-style-type: none"> <li>■ Government, regulators, industry and academia should reinvigorate research into standards for data sharing, including:                             <ul style="list-style-type: none"> <li>- formalising approaches for collecting and managing privacy metadata;</li> <li>- developing PIA processes that can take into account the privacy implications of sharing data across many different systems; and</li> <li>- defining acceptable information security controls for the exchange of personal information.</li> </ul> </li> </ul> <p>The ICO will be in a position to guide and support this work.</p> <ul style="list-style-type: none"> <li>■ Future awareness initiatives from the ICO and other relevant regulators should restate and promote principles of data minimisation across all organisations.</li> </ul>

Theme	Barriers to privacy by design	Desired privacy outcomes	Recommendations for delivering privacy by design
<b>Developing practical privacy standards</b>	<ul style="list-style-type: none"> <li>■ Organisations are often uncertain how to implement systems that comply with data protection law, and are left to manage privacy in accordance with 'best efforts', with each system approaching the issue on a case-by-case basis.</li> <li>■ There are no internationally-recognised standards to guide organisations in implementing privacy controls.</li> </ul>	<ul style="list-style-type: none"> <li>■ Organisations are able to operate in compliance with consistent, affordable, provable privacy standards, in much the way they already do with information security standards.</li> </ul>	<ul style="list-style-type: none"> <li>■ Government, regulators, industry and academia should be encouraged to develop practical standards for privacy implementation, supported by guidelines for the functionality and specific technologies that should be considered for incorporation into new systems. This initiative has to come from the organisations themselves so that they contribute and collaborate to ensure that resultant standards meet their needs. The work should not be in isolation, but rather should engage with similar emerging initiatives elsewhere. The ICO has a role to play in guiding and supporting the initiative.</li> </ul>
<b>Promoting privacy enhancing technologies</b>	<ul style="list-style-type: none"> <li>■ PETs have yet to find widespread adoption in 'real world' environments because organisations and vendors are fearful of committing to specific PETs in case these quickly prove to be obsolete as technologies develop. Web 2.0, cloud computing and service oriented architecture developments will most likely add further complexity to this problem.</li> </ul>	<ul style="list-style-type: none"> <li>■ Vendors are encouraged to incorporate PETs and privacy functions into their off-the-shelf systems and to promote these as selling points.</li> <li>■ Organisations adopt PETs into their systems where appropriate.</li> <li>■ PETs are recognised as valuable tools to support the management of personal information.</li> </ul>	<ul style="list-style-type: none"> <li>■ Government, regulators, industry and academia need to work together to support existing and future PETs research, and in particular encourage research into: <ul style="list-style-type: none"> <li>- mechanisms to simplify obtaining and managing consent, revocation and data minimisation;</li> <li>- 'privacy-friendly' identification and authentication systems; and</li> <li>- methodologies to test and prove the effectiveness of privacy controls in systems and across organisations.</li> </ul> </li> <li>■ Successful initiatives should be developed into practical standards, and buyers encouraged to demand better privacy functionality from vendors.</li> </ul>
<b>Managing compliance and regulation</b>	<ul style="list-style-type: none"> <li>■ The ICO lacks the necessary resources and powers to detect, investigate and where necessary enforce compliance through punitive sanctions. In consequence, individuals perceive organisations as unaccountable when privacy problems arise.</li> <li>■ Many organisations treat the DPA as 'just another compliance issue', which is not necessarily enough to ensure effective privacy management controls.</li> <li>■ Despite the ICO's guidance, organisations are sometimes uncertain about what constitutes personal information or what powers individuals have over that data.</li> <li>■ Privacy professionals operate in an unregulated environment where there are few recognised qualifications or accreditation bodies. This makes it hard for organisations to gauge the level of competence of the individual practitioner, or to trust that person's work.</li> </ul>	<ul style="list-style-type: none"> <li>■ Individuals know that organisations will be held to account for proper management of personal information.</li> <li>■ Organisations have a clear understanding of what information is considered to be personal and what powers individuals have over it.</li> <li>■ Privacy professionals are trained and accredited to known standards.</li> </ul>	<ul style="list-style-type: none"> <li>■ Regulators and government should explore the idea of obliging organisations to nominate an executive-level representative who will be held accountable for proper management of personal information.</li> <li>■ The government needs to recognise the realistic increased funding requirements of an empowered ICO that can both promote and enforce privacy practices.</li> <li>■ The ICO should examine whether there is a need for any further guidance on what constitutes personal information, and continue to deliver practical advice for organisations about what powers individuals have over their data.</li> <li>■ There is a pressing need for the development of a professional body for privacy practitioners (possibly under the aegis of an existing chartered body). The aim of this body will be to train, accredit and promote the work of privacy professionals. Clearly the ICO will have an important role in supporting this.</li> </ul>

# Part one: The privacy by design challenge

## Introduction

Consumer trust in the ability of public authorities and private organisations to manage personal information is at an all-time low ebb. A stream of high-profile privacy incidents in the UK over the past year has shaken confidence in the data sharing agenda for government with associated impacts on high-profile data management programmes, and businesses are having to work that much harder to persuade customers to release personal information to them.

Despite a host of high-profile investigations and reports into the problem, more needs to be done to develop a long-term strategy for personal information management that engages all sectors, reduces privacy-related risks, and inspires individuals to entrust organisations with their data.

This is where **privacy by design** comes in: the evolution of a new approach to the management of personal information that ingrains privacy principles into every part of every system in every organisation. The challenge is great, since the approach must be acceptable to public authorities, private organisations and consumers alike, and for it to succeed it must result in the evolution of a 'privacy by design ecosystem' in which all the stakeholders work together to build privacy needs into their data management lifecycle.

## Understanding privacy and data protection

Privacy is a complex concept that varies greatly between cultures, but is generally recognised to be 'the right to be left alone'. It is at the heart of any trust relationship involving an individual, whether that relationship is with another individual or an organisation. When an individual feels that his or her privacy has been invaded or abused – and this is often a subjective judgement – the trust relationship can be damaged or destroyed, which can cause significant harm to both individuals and organisations.

In Europe, information privacy has coalesced around the concept of data protection, which is the application of privacy principles to the processing of personal information. The UK Data Protection Act (DPA), which is an implementation of the EU Data Protection Directive, states that anyone who processes personal information must comply with eight principles, which make sure that personal information is, for example, fairly and lawfully processed, and adequate, relevant and not excessive. For many organisations, the data protection approach to privacy tends to be a compliance-driven process: public authorities are obliged to do so through their own regulatory mandates, and private organisations often view it as a compliance issue. This compliance-driven focus can result in a somewhat low-key, 'tick the box' approach to privacy management. Ongoing data loss incidents prove that this approach comes up short.

In consequence, organisations can fail to consider privacy in a broader context and therefore may not address key privacy issues, such as assessing information risks from the individual's perspective; adopting transparency and data minimisation principles; exploiting opportunities for differentiation through enhanced privacy practices; and ensuring that privacy needs influence their identity management agenda (since identity technologies are invariably needed to deliver effective privacy approaches).

## Privacy and identity

Privacy is intimately entwined with identity. Organisations use identity technologies to bind personal information to the individual: good approaches deliver greater anonymity and privacy for the individual, whilst poor approaches collect, duplicate and expose personal information. Organisations that fail to recognise the link between identity systems and privacy leave themselves vulnerable to data loss incidents. Privacy and identity should be addressed as part of the same agenda, and in this report the word privacy includes all the aspects of identity that have a privacy connection.

“Personal information, be it biographical, biological, genealogical, historical, transactional, locational, relational, computational, vocational or reputational, is the stuff that makes up our modern identity. It must be managed responsibly. When it is not, accountability is undermined and confidence in our evolving information society is eroded. It may very well be that our fundamental ideas about identity and privacy that we have collectively pursued and the technologies that we have adopted, must change and adapt in a rapidly evolving world of connectivity”

- Ann Cavoukian Ph.D, Information Commissioner of Ontario

## Ownership and control

At the heart of the current privacy debate is the key concept of ownership and control over personal information. Advocates argue that without control individuals cannot have real privacy: the individual should have control over use of their personal information, and using their own resources, or those of an independent third-party, be able to give, revoke or withhold consent for organisations to use this information.

## The future of privacy

Huge technology developments lie ahead. Web 2.0 offers potentially astounding capabilities, with almost unlimited access to programs, services, processing power and data storage – where the user will have no idea which computer, organisation or even country is involved. In this environment, privacy and identity management in particular will be the foundation of success. Without it the full benefits – for both individuals and organisations – will not be realised. Privacy by design is the way to meet this challenge.

## What is privacy by design?

The purpose of privacy by design is to give due consideration to privacy needs prior to the development of new initiatives – in other words, to consider the impact of a system or process on individuals' privacy and to do this throughout the systems lifecycle, thus ensuring that appropriate controls are implemented and maintained.

## Privacy by design in the systems lifecycle

For a privacy by design approach to be effective, it must take into account the full lifecycle of any system or process, from the earliest stages of the system business case, through requirements gathering and design, to delivery, testing, operations, and out to the final decommissioning of the system.

This lifetime approach ensures that privacy controls are stronger, simpler and therefore cheaper to implement, harder to by-pass, and fully embedded in the system as part of its core functionality. However, neither current design practices in the private and public sectors, nor existing tools tend to

readily support such an approach. Current privacy practices and technologies are geared towards 'spot' implementations and 'spot' verifications to confirm that privacy designs and practices are correct at a given moment within a given scope of inspection.

### **Use of privacy impact assessments (PIAs)**

Where the success of a project depends on people accepting, adopting and using a new system, privacy concerns can be a significant risk factor that threatens the return on the organisation's investment. In order to address this risk, it is advisable to use a risk management technique commonly referred to as a privacy impact assessment (PIA).

In 2007, the Information Commissioner published a PIA approach. This first step in promoting PIAs laid out what to do but not 'how' it should be done or what methods or processes are considered sound. A further positive step was taken in 2008 when the government made it mandatory to conduct a PIA on all new government systems that collect and process personal information (the Canadian government introduced such a mandatory ruling in 2003 and has promoted PIAs since<sup>1</sup>).

A possible criticism of the PIA is that it can be seen as overlapping with the many available processes for assessing information security requirements, but it is critical to take the PIA-driven viewpoint of the individual into account, something which few security risk assessment approaches do. It may, therefore, be more productive to integrate the two activities into a common risk assessment approach.

## **About privacy enhancing technologies (PETs)**

There is no widely accepted definition for the term privacy enhancing technologies (PETs) although most encapsulate similar principles. A PET is something that:

- reduces or eliminates the risk of contravening privacy principles and legislation;
- minimises the amount of data held about individuals; or
- empowers individuals to retain control of information about themselves at all times.

Today, there is a general understanding that PETs are consistent with good design objectives for any system or technology that handles personal information, and can offer demonstrable business benefits and competitive advantages for organisations that adopt them. PETs should not be 'bolted-on' to systems or technologies that would otherwise be privacy-invasive. Privacy-related objectives must be considered alongside business goals, and privacy considerations addressed at every stage of the systems lifecycle<sup>2</sup>.

### **Classifying PETs**

In the same way as there is no widely accepted definition for the term PETs, nor is there a recognised means of classification. Recently though, some studies have categorised PETs according to their main function as either privacy management or privacy protection tools<sup>3,4</sup>.

---

<sup>1</sup> [http://www.privcom.gc.ca/pia-efvp/index\\_e.asp](http://www.privcom.gc.ca/pia-efvp/index_e.asp)

<sup>2</sup> Dr Steve Marsh, Dr Ian Brown, and Fayaz Khaki. Privacy engineering whitepaper. <http://tinyurl.com/5zv9b3>

<sup>3</sup> Lothar Fritsch. State of the art of privacy-enhancing technology (PET). <http://publ.nr.no/4589>

<sup>4</sup> The META Group. Privacy enhancing technologies. <http://tinyurl.com/6h3qrq>

## Privacy management tools

Privacy management tools enable the user to look at the procedures and practices used by those who are handling personal information. They may also advise users of the consequences of the information processing performed leading to an improved understanding of privacy-related issues. There are a limited number of tools in existence today that cater for either the enterprise or the end-user market: examples include P3P<sup>5</sup> and IBM's secure perspective<sup>6</sup> software.

## Privacy metadata

Widespread adoption of user-centric identity management (U-Idm)<sup>7</sup> platforms, and indeed most other PETs, will depend upon the existence of standard ways to describe our personal information and the manner in which it may be processed by information systems. This is generally achieved by attaching to information tags called metadata: additional information that details the likes of its source, the consent obtained, how it may be used, and the policies to which it is subject. The personal information may also be accompanied by a set of conditions, known as obligations, covering such things as the length of time that the data may be retained or whether the user's consent is given for passing the information to third parties.

Work is underway in the research community to investigate detailed metadata requirements and to encourage use and dissemination of standards through bodies such as W3C's Policy Languages INterest Group (PLING)<sup>8</sup>.

## Privacy protection tools

Privacy protection tools aim to hide the user's identity, minimise the personal information revealed and camouflage network connections so that, for example, the originating IP address is not revealed. By learning the IP address an observer may be able to pinpoint the user's geographic location to the nearest town or city or even uniquely identify the computer. Privacy protection tools may also authenticate transactions such as payments while making it impossible to trace a connection back to the user. Some of the software that falls into this category includes:

- **Anonymising tools:** PETs in this category hide the IP address of the originator and, in the case of anonymous or pseudonymous mail, the source email address. Some 'anonymous remailers', such as Mixminion, employ sophisticated techniques that enable receivers to reply to messages. More generally, Tor is a network of virtual tunnels on the internet that individuals and groups can use to keep websites from tracking them, to connect to news sites, instant messaging services or similar network services when these are blocked by their internet service providers or may be sensitive in nature. A Firefox add-on, the Torbutton, provides a way to securely and easily enable or disable the browser's use of Tor at the click of a mouse. Microsoft's Internet Explorer 8 will incorporate 'InPrivate'<sup>9</sup> functions to deliver similar privacy outcomes.
- **Anonymous or pseudonymous payment:** The concept behind anonymous payment is straightforward and usually works in this way: the user purchases a pre-paid card that is identified by a unique number. When the user makes a purchase at an online store, payment is retrieved from the anonymous cash provider using the unique number on the card. Successful examples of commercial pre-paid cards include Paysafecard in Europe.

---

5 <http://www.w3.org/p3p/>

6 <http://tinyurl.com/6528k4>

7 <http://www.youtube.com/watch?v=RrpajcAgR1E>

8 <http://www.w3.org/Policy/pling/>

9 <http://tinyurl.com/6nl26k>

- **Information security tools:** There are a number of applications for the end-user that are sometimes categorised as PETs but can equally be considered to be information security tools. Such tools are important to data protection and privacy but the primary goal is usually more modest: that of preventing unauthorised access to systems, files or communications over a network. For example, most web-server and browser software can encrypt communications using the TLS or SSL protocol and this feature has been a significant factor in increasing confidence in online banking and e-commerce services.

## The future of PETs

Technological advances are increasing apace and there is no doubt that PETs can provide a way of harnessing these technologies to protect privacy. The need to minimise the collection and processing of personal information, and to design systems around that principle, will be supported by privacy-friendly identification and authentication mechanisms. PETs researchers agree that there is a need for the will to design systems in a privacy-friendly manner, and for enterprise developers and software vendors alike to incorporate PETs into their system designs.

In the near future, research into user-centric identity management (U-Idm) frameworks may represent a solution to the secure control and management of personal information. In most U-Idm frameworks users manage their own personal information which is stored on a personal computer or handheld device that they control. U-Idm could facilitate update of, say, address information to multiple parties or provide proof of age or proof of entitlement online without revealing unnecessary identifying details. An important milestone for this is Microsoft's recent acquisition of Credentica's U-Prove technology which exploits special cryptographic techniques enabling users to enforce data minimisation or prove certain characteristics. Microsoft intends to embed these features in its U-Idm software, Windows CardSpace.

## The challenge for privacy by design

Despite the many developments in both PETs and other related security technologies, the slew of recent data loss incidents shows that privacy principles are not always reflected in the design of systems and associated business processes. Progress in the development of privacy-friendly systems has been disappointing, and there is a clear sense that both public authorities and private organisations could be doing more to protect individuals' privacy.

A consequence of this failure to achieve privacy by design is a breakdown in relationships between individuals and public/private organisations. An environment is developing in which there are constant tensions between individuals and organisations, with a sense that privacy is subservient to the financial value of personal information (complaints about DVLA providing information to parking enforcement companies for a fee). As a result, individuals feel that they have insufficient knowledge of how their data is used, but they are aware from media reports and notifications that their data is being lost. When this happens, those responsible have rarely appeared to be held accountable for their actions.

"I dread to think how much information is out there about me"  
- Attendee, Privacy by Design workshop

There is a widespread perception that organisations fail to minimise the amount of data that they collect or retain. This has created an environment where public authorities and private organisations

demand increasing amounts of information to offer services, and retain it for long periods, without providing a clear statement about the proportionality of that processing to the individual. Relationships with individuals have been 'poisoned' since some people now see it as acceptable to lie or withhold information from a service provider in order to obtain the service they are legitimately entitled to without having to hand over excessive personal information.

The challenge for privacy by design will be to achieve a cultural, management, technological and regulatory environment that can effectively address these problems and promote the broader use of PETs to protect privacy.

# Part two: Barriers to privacy by design

## Introduction

Privacy by design is an approach that will go a long way towards addressing the privacy-related tensions between individuals and organisations. However, there are management, process and technology ‘barriers’ that will prevent the evolution of a more productive privacy environment. These must be removed if privacy by design is to succeed.

## Lack of management engagement

At the heart of individuals’ concerns about processing of personal information is a perception that there is a lack of rigorous processes, failure to recognise organisations’ responsibilities for privacy management, and a lack of accountability at senior management levels for the proper handling of personal information, despite the high-profile data loss incidents of recent times. There are a number of significant barriers that contribute to this situation.

### Attitudes towards privacy and data protection

A cultural barrier to privacy by design arises in attitudes toward the Data Protection Act (DPA). Many organisations see the DPA as the maximum requirement for privacy rather than the minimum, and look to the law to tell them what they can’t do rather than what they can, leading to disputes about what constitutes morally acceptable use of personal information. Often these organisations view the Act as ‘just another compliance issue’<sup>10</sup>, and leave compliance to the relevant department rather than encouraging an organisational culture in which respect for privacy is valued.

Some organisations treat privacy as a function of information security, which can lead to failures to respect privacy needs. For example, the Poynter review of data losses in HMRC<sup>11</sup> explores the causes of the biggest loss of personal data in UK history, yet at no point in the document does it mention the word ‘privacy’, but instead treats the problem as a systemic security failure.

The consequence of these issues is that executive managers do not always recognise their duties for privacy management, and hence often fail to create an organisation-wide culture that respects the rights of individuals.

### The language of privacy

The difficulty of defining privacy needs has already been explored; but an equally significant problem is that of expressing the highest level requirements in a way that does not undermine privacy principles.

The language of privacy and identity is complex and whilst taxonomy is developing<sup>12</sup>, there are still disagreements, even between privacy professionals about how to describe privacy-related concepts. This lack of a shared vocabulary to discuss privacy and identity issues, compounded with a lack of awareness of what is required, means that system owners and executive managers all too often issue

---

<sup>10</sup> <http://tinyurl.com/6rawoa>

<sup>11</sup> [http://www.hm-treasury.gov.uk/poynter\\_review%20.htm](http://www.hm-treasury.gov.uk/poynter_review%20.htm)

<sup>12</sup> <http://tinyurl.com/5lec7d>

and sign-off system specifications that fail to address privacy satisfactorily. For example, they confuse 'identification' with 'authorisation' or 'verification', resulting in systems that capture personal information that simply isn't needed.

### **Uncertain benefits of privacy management**

For the majority of organisations, the benefits case for offering privacy, and in some cases for meeting the basic compliance needs of the DPA (particularly outside of regulated or publicly owned organisations), is unclear. This makes it very hard to justify investment in privacy functionality for new systems.

Indeed for some businesses there would an argument – albeit not a legitimate one – that it could be cheaper to 'just not do it'. By gathering and retaining as much data as possible the business has a perception that it may receive likely benefits such as future data mining and marketing opportunities, despite the 'toxic liability' that may arise from holding this information. This is because the risks of legal or regulatory action arising from data loss incidents remain minimal. Traditionally, sanction imposed by courts or the ICO tend not to be punitive, and the cost of a fine is unlikely to be as great as that of implementing a compliance regime. Clearly this is not a morally or legally acceptable approach, but the reality is that it is one that some businesses do take.

Whilst personal information is perceived by businesses as a valuable commodity, with few risks associated with holding it, this state of affairs is likely to continue.

#### **Key points:**

- Executive managers don't always recognise or correctly prioritise their organisation's responsibility or their own accountability for protecting individuals' privacy.
- Executives and their staff often lack a shared language to discuss or to specify privacy requirements in a clear unambiguous way. As a result, poor privacy specifications deliver poor privacy controls.
- Commercial risks and benefits of managing personal information are often unclear, making it hard to justify privacy investment. In consequence privacy needs are often omitted from the business cases for new systems.

## **Failure to plan for privacy in the systems lifecycle**

Even when an organisation's executive management issue a clear mandate to adopt privacy-friendly practices, an important barrier to privacy by design is the ability to incorporate privacy issues into organisational risk assessment and management processes. Security risk assessments – of which there are many – rarely take into account the needs of the individual and often fail to assign meaningful threat values to the loss of personal information, so the risks associated with such incidents are not properly managed. Similar problems exist in security standards such as ISO27001 that do not take into account risks from the individual's perspective, nor do they prescribe privacy controls.

"Risk assessment processes haven't kept pace with technology.  
You try losing 25 million paper files."  
- Attendee, Privacy by Design workshop

This often means that assessments fail to identify these non-functional or 'hidden' requirements and thus the need for appropriate privacy controls. In other words, system owners fail to specify them because they are either unaware of the need, or assume that they will be dealt with automatically at some point in the development lifecycle (this situation being similar to security in the past, where designers would often take the attitude that "the operating system has security controls so I don't need any").

In such an environment, organisations do not often demand privacy functionality from system vendors, or weight it highly when assessing 'off-the-shelf' software. As a result, vendors have little incentive to build privacy functions into their systems.

Furthermore, for many organisations assessments aren't continued beyond the system specification stage. Systems are commonly assigned new tasks (often referred to as 'function creep'), original objectives often fail to be clear or auditable, and data such as account details, challenge/response questions and scanned signatures spread beyond systems and organisations, where individuals' control over that data is lost.

### **When privacy functionality is omitted from the system design**

An important example of what can happen when privacy functionality is not properly considered is that of transparency. The DPA mandates the right of individuals to access their personal information held by data controllers, a process that is achieved through a subject access request (SAR). A request is typically submitted by sending a letter to the data controller, together with a payment of no more than £10. The request allows individuals to see what data is held on them and what is being done with it, and is a keystone of transparency in personal information processing.

However, problems can arise when systems have not been designed with functions to identify the presence of personal information about a given individual, or where an organisation operates numerous diverse systems containing distributed or even duplicated data. A lack of automated SAR functionality can greatly increase the cost to the organisation of servicing the request, and there are success stories from organisations that have not only addressed, but have in fact automated, their SAR process: for example, some credit reference agencies have fully automated their SARs with online applications for individuals<sup>13</sup>.

### **The privacy impact assessment (PIA)**

The ICO Privacy Impact Assessment Handbook is an important step forward to address privacy needs in the systems lifecycle, but unless an organisation has incorporated the process throughout its project lifecycle, privacy risks are unlikely to be adequately managed.

Within government circles, concerns have been raised that the PIA appears to duplicate work already present in the risk management accreditation document set (RMADS) that is mandatory for all new systems, and the exact nature of how the two processes should be integrated appears unclear to many practitioners. Further guidance in this area would be of benefit to all parties.

---

<sup>13</sup> <http://www.wiseconsumer.uk.experian.com/>

**Key points:**

- Traditional risk management methodologies often fail to consider the value of personal information, and hence do not take privacy needs into account.
- Risk assessment approaches often fail to manage privacy needs throughout the systems lifecycle, so many bespoke and off-the-shelf systems are still built without proper or innovative privacy controls.
- Privacy needs are often not rigorously considered at any stage of the systems lifecycle, so systems can be modified or re-used without consideration for privacy implications.
- Systems do not always support automated subject access requests, and hence information retrieval procedures can be onerous for organisations.

## Balancing data sharing with privacy needs

The pressure to share personal information both within and outside of organisations is compelling: internal efficiencies, enhanced marketing and the commercial value of personal information all drive the data sharing agenda in private organisations and public authorities. However, more often than not it is data sharing that causes major privacy breaches. Data can be lost when copies are transferred between systems using unencrypted physical media such as CDs or memory sticks, yet many organisations still see this as a workable solution to the data sharing agenda.

Government must accept a degree of responsibility for this attitude, since the most serious breaches have been within public authorities. When data losses happen in the public sector, they are often on such a large scale that the loss is too big to quantify in any meaningful way. Data of this scale has a great potential value to criminals, and losses are likely to have a long 'afterlife' when so much data is involved since much of it will remain usable for a long time. Public sector bodies traditionally often didn't apologise for losses; private sector organisations are perceived as being quicker to change their ways and offer compensation or apologies to affected individuals.

### Silos and systemic problems

The data sharing agenda has the potential to undermine privacy controls in those systems that have otherwise handled privacy issues in a meaningful manner. Perhaps the most important technology issue is that of operating multiple systems as 'data silos' without taking into account the broader systemic implications of many silos across one or more organisations, and the combined impact of those silos on private information.

If a single system is built in accordance with good privacy principles derived from a PIA, and incorporates necessary privacy controls and technologies, it may be capable of protecting personal information. However, if the organisation operates multiple systems, each of which has been designed in isolation, then it will have multiple silos of personal information. In all likelihood, not all of the systems concerned will have been built in accordance with good privacy practices, and will need to share data for the organisation to deliver its necessary processing outcomes. This means that the 'privacy-friendly' system shares information with other systems that do not incorporate such controls, and the data becomes vulnerable as soon as it passes to those systems. Few organisations – even those that have incorporated PIAs into their system operations – take this overall systemic impact into account when considering privacy risks.

## The loss of privacy metadata

Systemic issues also impact the value of privacy ‘metadata’ – data about personal information, such as when it was collected, from what source, with what expiry date, and with which usage permissions from the individual. This is essential information for nearly any privacy-friendly system to manage personal information in accordance with the wishes of the individual.

However, as data is shared between systems, privacy metadata may be lost since the non-compliant systems may have to strip the metadata in order to process the information. Those new systems are unable to fulfill the privacy wishes of the individual; nor is any subsequent system with which it shares the data; and that data will exist thereafter without any privacy metadata that could be used to rebuild the privacy needs of the individual.

## Data sharing or data aggregation?

One of the key privacy problems – particularly in government – that arises from the data sharing agenda is a confusion between ‘data sharing’ and ‘data aggregation’. Very often, instead of creating an index that facilitates cross-referencing between existing databases, it is deemed simpler to create a new, larger database containing aggregated data. Potential consequences of this centralisation of databases include duplication of personal information; increased risk of inaccurate or inconsistent data; loss of control over where data resides; increased data processing and storage costs; and a lack of transparency of processing that can have regulatory consequences.

## Confusing identifiers with indices

The Transformational Government agenda<sup>14</sup> calls for personalised service delivery facilitated by technology, but for many legacy systems this target will require the collection and maintenance of large volumes of (often duplicated) personal information. Data such as name, date of birth, national insurance number are used as indices – and in many cases as the primary identifying credentials – in many systems. This may facilitate data sharing but also renders the systems vulnerable to identity-related fraud. Ironically the personal information often isn’t necessary for service provision, but in the absence of sharing between legacy systems has to be recorded time and again. The ‘Tell Us Once’ project<sup>15</sup> aims to reduce this problem, but it will take many years before the thousands of affected systems can be updated. Until services such as the Government Gateway<sup>16</sup> are both operational and interfacing with systems across government this state of affairs is likely to continue.

### Key points:

- The pressure to share personal information within and outside of organisations can lead to privacy-related problems:
  - data from ‘privacy-friendly’ systems are shared with other systems that are less able to respect privacy needs;
  - copies of personal information in transit are not always appropriately secured;
  - organisations often aggregate data rather than sharing it;
  - identifiers are used as indices, making it hard to anonymise data thereafter;and
- privacy metadata can be lost as information is shared between systems.
- If system PIAs are conducted in isolation the results may fail to take into account the broader systemic implications of data sharing.

<sup>14</sup> <http://tinyurl.com/5v6frp>

<sup>15</sup> <http://tinyurl.com/5z6uzx>

<sup>16</sup> <http://www.gateway.gov.uk/>

## The need for privacy standards

For any organisation that is implementing privacy practices, whether for baseline compliance with the DPA, or a more rigorous privacy regime, a fundamental challenge is the absence of internationally recognised privacy standards and associated best practice guidelines and development standards.

The DPA, and similar legislation around the world, define the privacy outcomes that are required without providing guidance on how to achieve it. Whilst it is clearly not the role of legislation to define such guidelines, standards are important for businesses. Inconsistent interpretations of the EU Data Protection Directive in each member state, a fundamentally different approach to the protection of personal information in the US, and the extra-territorial nature of some laws (eg California) mean that organisations have a wealth of international laws with which to comply. Many of these conflict with each other, and it is extremely difficult to track the changes worldwide.

Some excellent standards exist, such as those published by the Canadian Institute of Chartered Accountants<sup>17</sup>, but none that are yet internationally recognised (the British Standards Institute<sup>18</sup> and ISO/IEC<sup>19</sup> have ongoing projects in this field). Most importantly, whilst some data protection laws (Spain) dictate certain security requirements to comply with security principles of the DPA, there is no widespread recognition of what constitutes an acceptable level of security for the protection of personal information.

This situation leaves organisations in a difficult position, as they are unable to confirm what constitutes compliance with data protection laws, and need to implement their compliance efforts on a case-by-case basis. It becomes hard for executive management to be certain that the organisation has achieved compliance (particularly since auditors have no baseline against which to confirm as such), and even when it has there remains the risk that if an incident occurs then an investigation may judge security controls over personal information to be inadequate.

### Designing for privacy

As a result of the lack of recognised standards, the privacy controls within any new system or process largely depend on a number of factors:

- the organisation's overall privacy or data protection policy (if any);
- whether or not the organisation has adopted a PIA into its systems lifecycle;
- the privacy awareness and capability of the system owner and individual designers;
- the complexity, schedule and budget for the system (which may deter the wish to introduce privacy controls – often seen as an additional complexity – into the programme); and
- the regulatory environment in which the organisation operates (eg financial service organisations will have to implement controls in order to comply with their regulators).

In the absence of specifications, developers are left to use common sense, their interpretation of the DPA and their own perception of social responsibility, and in such circumstances it is highly unlikely that developers will interpret individuals' wishes in a rigorous or accurate way. This can be contrasted with information security, where there are numerous detailed standards available, secure development methodologies and recognised security testing and audit mechanisms. Whilst it seems unlikely that a universal privacy standard will be achievable in the short or even medium-term, the complete absence of such standards is clearly a hindrance to a privacy by design approach.

**Key points:**

- Organisations are often uncertain how to implement systems that comply with data protection law, and are left to manage privacy in accordance with 'best efforts', with each system approaching the issue on a case-by-case basis.
- There are no internationally-recognised standards to guide organisations in implementing privacy controls.

## The problems with PETs

Rapid technology developments make it very difficult to develop and agree standards for PETs. In consequence organisations are nervous about adopting the technologies, for fear of introducing unnecessary project complexity, risk, or investing in a technology that later proves to be obsolete. Legacy systems cannot be updated easily, and where new systems incorporate privacy protection, the associated technologies and metadata are often incompatible with older systems.

The move towards Web 2.0 and service oriented architectures (SOA), coupled with the emergence of cloud computing<sup>20</sup>, has further complicated the environment for PETs: traditional data models are no longer relevant, the location and ownership of personal information becomes unclear, and the new relationship between organisations and vendors is not clearly understood by all parties concerned. Where software and storage are being procured as a service, rather than an in-house function, it can be unclear who is responsible for managing privacy controls, and where the resultant accountability rests. PETs are not going to be developed and deployed in this environment without a fresh catalyst for their usage.

**Key points:**

- PETs have yet to find widespread adoption in 'real world' environments because organisations and vendors are fearful of committing to specific PETs in case these quickly prove to be obsolete as technologies develop. Web 2.0, cloud computing and SOA developments will most likely add further complexity to this problem.

## Regulating privacy

Finally, a key barrier to privacy by design is the regulatory/compliance environment. Certain industry sectors (eg financial services) that regularly handle large volumes of sensitive personal information are subject to stringent regulatory controls and associated punitive sanctions from their respective regulators if they fail to comply. However, the majority of organisations are not subject to any privacy enforcement mechanism other than the requirements of the DPA and the powers of the ICO. Unfortunately, the ICO has in the past had insufficient resources to detect, investigate and prosecute organisations that openly disregard and breach the DPA, let alone to pursue those that are operating in a manner that may be legal but is not acceptable to individuals.

### Good compliance does not ensure good privacy

In organisations that are not subject to sector-specific privacy regulation, it is quite possible to attempt to comply with the DPA without in fact protecting privacy – for example, to submit a 'blanket' data controller registration and provide a fair processing notice which allows for unrestricted sharing and use of collected information. Such an approach can be a particular problem in large organisations which provide a single fair processing notice but use

<sup>20</sup> <http://tinyurl.com/5vvc74>

this to share personal information throughout the organisation for a multitude of purposes. In such cases, internal data sharing is not viewed in the same way as sharing outside of the organisation.

There is also a problem – particularly associated with public authorities – of information being collected under statutory authority or where there is ‘enforced consent’, since individuals have little option but to offer their consent if they are to obtain essential services such as social security payments, the right to drive or watch television, collection of their refuse, or access to healthcare. Such organisations have a far greater moral duty of care over the information they collect, even where consent has been ‘freely given’. Mere compliance with the DPA is not enough in these circumstances.

### **Defining personal information**

Despite guidance and clarification from the ICO, a further legal barrier to implementing privacy by design is uncertainty about what constitutes personal information.

For example, the IP addresses used by individuals’ PCs may be considered not to be personally identifiable, except where the data controller has access to other information that might enable cross-referencing of the address<sup>21</sup> against other information to identify the likely holder of the address. Privacy advocates argue that these addresses are identifiable. This lack of certainty has been a contributing factor to the debate over the acceptability of online behavioural profiling systems such as Phorm<sup>22</sup>.

### **Ownership of personal information**

Another area of significant legal confusion is that of ownership of personal information. It is generally accepted that where personal information is gathered by an organisation, that information is the property of the organisation concerned, although it remains subject to the stipulations of the DPA. However, the issue of who should have control over the personal information is not always clear.

### **Privacy professionalism**

It is also widely acknowledged that conventional risk assessment approaches are only as good as the practitioners who use them, yet there are few recognised qualifications for privacy professionals, and few individuals who hold the relevant qualifications, leaving organisation uncertain about whether their privacy practitioners are actually competent to do the job. This also makes it difficult to compare assessment results between projects or organisations, since there can be little confidence that the practitioners concerned share the same skill sets.

The information security profession has been through this same problem, and is now engaged in the establishment of a range of professional qualification, accreditation and regulation activities.

#### **Key points:**

- The ICO lacks the necessary resources and powers to detect, investigate and where necessary enforce compliance through punitive sanctions. In consequence, individuals perceive organisations as unaccountable when privacy problems arise.
- Many organisations treat the DPA as ‘just another compliance issue’, which is not necessarily enough to ensure effective privacy management controls.
- Despite the ICO’s guidance, organisations are sometimes uncertain about what constitutes personal information or what powers individuals have over that data.
- Privacy professionals operate in an unregulated environment where there are few recognised qualifications or accreditation bodies. This makes it hard for organisations to gauge the level of competence of the individual practitioner, or to trust that person’s work.

21 <http://tinyurl.com/yvvg98p>

22 <http://tinyurl.com/5m69mx>

# Part three: Delivering privacy by design

## Introduction

This section considers the actions that will be needed to deliver privacy by design. Principles of obtaining executive support; incorporating privacy controls into every stage of the systems lifecycle; addressing privacy needs within the data sharing agenda; developing privacy standards; promoting PETs; and overseeing the process through an empowered and properly-resourced regulator will all be necessary to put these recommendations into practice.

## The privacy by design ecosystem

At the heart of the success of privacy by design will be the creation of a 'privacy by design ecosystem' – an environment that engages all stakeholders at all levels across all sectors to ensure that privacy becomes embedded not only in all aspects of the systems lifecycle, but for organisations becomes part of 'the way we do things around here'. A successful privacy by design ecosystem will encourage organisations to invest in PETs and privacy-friendly systems.

At present such an ecosystem does not exist, and hence privacy needs are often driven out of the systems lifecycle – unclear benefits and a low risk of enforcement mean that organisations tolerate poor compliance regimes, and they do not prioritise privacy in their systems, leading to low demand for privacy solutions, and hence vendors are not under pressure to deliver PETs in their products.

However, in a more constructive environment, government and major corporates would mandate the requirement for privacy controls in their systems, and work with vendors to agree suitable design standards; once in place, they would then call upon their suppliers to conform with these standards, and this would propagate through the procurement chain. Once vendors have 'off the shelf' products that incorporate these standards, they will be available to all public authorities and private organisations.

Within each organisation, the mandate will need to spread down from executive management throughout the organisation, being delivered as policies, standards and implementation guidelines, and then reported back through audit processes.

This outcome cannot succeed without the support of the major system integrators and software vendors who have the ability to provide products and services that support privacy by design. This will require mutual agreement not only with the UK divisions of those companies, but the international (predominantly US) parent companies to ensure that they take into account these ideas in their global product development.

## Learning lessons: How security by design succeeded

The current status of privacy echoes that of information security some 20 years ago, when the subject was poorly understood and often overlooked in the development of information systems. Today, however, information security is recognised as an important topic in both the commercial world and government, and information security requirements are built in to most major information systems as a matter of course. What lessons can be learned from how this transformation came about?

The following table describes the key factors that contributed to security by design, and suggests how these might apply to privacy by design.

Key factors in security by design	Lessons for privacy by design
<p><b>Understanding the threat</b></p> <ul style="list-style-type: none"> <li>■ Growth of the internet and e-commerce significantly raised the risks.</li> <li>■ Major incidents and the activities of hackers raised awareness.</li> <li>■ Reliable statistics on incidents became available.</li> <li>■ The business case for information security investment became convincing.</li> </ul>	<ul style="list-style-type: none"> <li>■ Privacy risks have increased substantially – identity-related fraud is one of the fastest growing crimes globally – but this has not been communicated effectively.</li> <li>■ Further work is required on gathering reliable statistics, clearly expressing the threats, highlighting the benefits of addressing privacy at the start of a project and developing sample business cases.</li> </ul>
<p><b>Management standards</b></p> <ul style="list-style-type: none"> <li>■ Recognition that management issues are as important as technical issues.</li> <li>■ Significant activity in developing information security management standards – BS 7799 (UK), ISO/IEC 17799 (International).</li> </ul>	<ul style="list-style-type: none"> <li>■ Recognise that privacy is a management issue as much as a technical issue.</li> <li>■ Effective privacy standards should be actively pursued, preferably at international level.</li> </ul>
<p><b>Executive awareness</b></p> <ul style="list-style-type: none"> <li>■ Significant work undertaken by national and international bodies in the area of corporate governance – 18 major reports, guidance and legislation between 1986 and 2002 such as Sarbanes Oxley Act (USA).</li> <li>■ This work stressed the need to evaluate risks and apply controls and served to legitimise information security as a topic of concern for senior management.</li> </ul>	<ul style="list-style-type: none"> <li>■ Privacy is recognised as an important element of corporate governance but there is little evidence that this has been used effectively to gain executive attention.</li> <li>■ Further work is required to show the clear link between privacy and corporate governance and to communicate it widely and in particular to senior executives.</li> </ul>
<p><b>Language and frameworks</b></p> <ul style="list-style-type: none"> <li>■ Based on clear definitions there was a growing consensus on the definition and scope of information security.</li> <li>■ At national and international level, information security professionals can communicate effectively.</li> <li>■ Other disciplines such as internal audit agree with definitions which makes cooperation more successful.</li> </ul>	<ul style="list-style-type: none"> <li>■ There is no widely accepted definition of privacy – a particular problem with so many different parties involved in achieving privacy. There is also no widely accepted description of the relationship between privacy, identity and information security.</li> <li>■ There is an urgent need for clear definitions and for agreement among the parties involved.</li> </ul>
<p><b>Organisation and responsibilities</b></p> <ul style="list-style-type: none"> <li>■ Chief Information Security Officer (CISO), appointed in most major organisations, acts as a focus point and provides knowledge and expertise.</li> </ul>	<ul style="list-style-type: none"> <li>■ The appointment of a Chief Privacy Officer (CPO) at an appropriately high level of seniority should be encouraged and recommended as good practice.</li> </ul>

The following pages describe the objectives and recommendations for delivering the privacy by design ecosystem.

# Part four: Recommendations for delivering privacy by design

## Introduction

This section provides specific recommendations for delivering privacy by design. These are not intended to be comprehensive, complete or prioritised, but rather to provide a framework for the further development of plans to implement privacy by design. The ICO will be in a position to develop these points, exploring the key issues in greater detail, refining recommendations and putting them into practice.

## Engaging executive management

The first critical step in delivering privacy by design will be to engage with, and obtain support from, senior executives in public authorities and private organisations.

### Desired outcomes:

- Executive managers understand their privacy duties and communicate their privacy management wishes across the organisation.
- Business cases for new systems incorporate privacy specifications that are understood by all members of staff.

## The mandate for privacy by design

The first step in obtaining executive commitment will be to build a mandate for privacy by design: a popular call from across government and industry bodies, including the ICO and other sector-specific regulators, to adopt privacy by design. The call should be for organisations to recognise that privacy issues are an important component of the corporate governance agenda, to incorporate privacy controls into all new systems, and to fit them into existing systems as they are maintained and modified. Where business cases for new systems are presented without a supporting PIA, they should be rejected. This is a logical and beneficial step, since a PIA may reveal a need for additional controls or even a fundamentally different approach, with consequential costs for the project. In the public sector, this approach could be mandated for all systems.

## Demonstrating benefits of privacy by design

Businesses in particular need to understand the importance of privacy by design, and its potential impact on the bottom line. This could be achieved by providing example benefits cases that clearly express the possible commercial benefits of a privacy-friendly customer offering, whilst demonstrating the risks associated with poor privacy practices.

## Creating a language for privacy by design

The ICO has worked hard to promote awareness of data protection, with a considerable degree of success. Efforts now need to focus on the language of privacy, with a goal of equipping executives and technology professionals with a shared vocabulary that allows them to discuss privacy requirements in a clear and unambiguous manner.

This approach should focus on desired outcomes – such as proportionality of collection, data minimisation or transparency of processing – rather than the functions used to implement privacy controls. The language must be meaningful to executives and avoid technology where possible.

The clarification of a common language should also be promoted within legal circles with the objective of simplifying online privacy policies and fair processing notices. Only when lay individuals can quickly and easily understand fair processing notices will they be able to actually make informed decisions about processing of their personal information.

#### **Key recommendations for privacy by design:**

- The executive managers of public authorities and private organisations need greater awareness of their privacy responsibilities, and this should be supported by:
  - providing sample costs, risks and benefits cases to demonstrate the value of privacy compliance; and
  - promoting a simple shared language for key privacy concepts such as data minimisation, identification, authentication and anonymisation to assist communication within and outside of organisations.

The ICO and other regulatory bodies have a role in making this happen.

## **Planning for privacy by design**

Delivering privacy by design in the organisation will require a structured framework of processes and technologies that can deliver the relevant policies and standards mandated by the organisation's executive management.

#### **Desired outcomes:**

- Systems incorporate appropriate PETs based upon a rigorous privacy impact assessment.
- Privacy needs are managed throughout the systems lifecycle.

### **Privacy impact assessments (PIAs)**

PIAs are intended to identify privacy-related risks from the earliest stages of a project onwards, so that privacy issues can be addressed within the system design and safeguards incorporated rather than being added later on.

Throughout this process the organisation must understand its own 'risk appetite' – ie what degree of failure is considered an acceptable risk? For example, a system that only leaks or loses a single financial transaction in every 10 million might be considered acceptable from the organisation's perspective, but not to the individual concerned. A balance needs to be struck whereby privacy-related failures are reduced to a reasonable level.

All projects have to balance cost, quality and time, and invariably are limited on each. Project managers have to understand how the organisation wishes to prioritise privacy needs over other competing requirements, guided by a high-level policy statement that defines the baseline tolerances.

Therefore the first operational step for privacy by design should be to ensure that the organisation has an overall PIA or equivalent privacy policy to define baseline risk tolerances and appetites, and that this forms the template for incorporating PIAs into all new systems and system changes. In the case of the public sector, this should include assessments that span authorities and departments, and might even include a pan-sectoral assessment.

When delivering system-specific PIAs, it is important that practitioners go much further than simply a data protection law compliance check (although this should of course be part of the process). The assessments need to consider all aspects of privacy, from the perspective of the individual rather than the organisation. This clearly may appear to be onerous, but with the ICO's recommended approach it should be possible to conduct a simple, high-level assessment to ascertain whether there is a need for greater investigation (for example, to identify whether a system holds sensitive personally-identifiable information), and then to initiate more detailed investigations if necessary.

In the case of critical systems – such as those processing very sensitive personal information, extremely large volumes of personal information, or with a high number of security risks (such as many distributed users) – the organisation should consider providing a copy of the PIA to the ICO for verification. In such cases it would be reasonable to expect the ICO to grant a degree of tolerance to those organisations that suffer privacy-related incidents but have taken all reasonable steps to transparently deliver a privacy by design process.

### Transparency of PIAs

If an organisation has delivered a PIA, then a valuable step to demonstrate commitment and transparency would be to place that document in the public domain – a logical step, since it relates to the individuals' information. For the public sector, this approach could be mandated for all PIAs, thus demonstrating both the commitment to PIAs and the existence of the documents on a per-system basis.

### Introducing system transparency through subject access requests

If systems incorporate subject access request (SAR) functionality at the design stage, then as well as providing essential functions for the business, they will encourage system architects to adopt a more individual-centric approach to their data definitions. It is, therefore, in the interests of both organisations and individuals to ensure that systems are designed to automatically service SARs.

In order to deliver an environment where this is possible, five key issues need to be addressed:

- **Mandate:** Public-sector organisations should mandate that all new systems that process personal information must support SAR functionality (although it should not be mandatory to offer online subject access). Similar mandates from the regulators of private-sector organisations – particularly in the financial services sector – would force the incorporation of functionality into the commercial environment.
- **Clarification:** There can be considerable legal uncertainty about what constitutes personal information, and organisations will need greater clarification if they are to be able to design SAR functionality into their systems.
- **Authentication:** There is a mutual challenge for organisations and individuals in submitting SARs, since the individual has to prove his/her entitlement to access the data. In the majority of cases this requires a written request for the data to be sent to the address held on file, but this model does not work if the individual has not disclosed his/her address to the organisation (eg certain online services) or if the request in fact relates to data where there is no existing relationship (eg where an

organisation has received data from a third party but has had no previous contact with the individual). Organisations need to reconsider their use of strong authentication techniques in order to facilitate the SAR process and to assure all parties that data will only be released to a legitimate requesting party.

- **Promoting online subject access:** A coordinated strategy for offering online SARs is an important long-term goal. On a sector-by-sector basis, public authorities and private organisations need to develop targets for moving towards simple online delivery of data when it is requested.
- **Intolerance of non-compliant systems:** Where an organisation has difficulty fulfilling a SAR because it feels it to be excessive or disproportionate, if part of the reason is that its systems do not support the request then that should not be a permissible excuse.

Organisations should be urged to ensure that their new systems incorporate this functionality as a means to introduce and prove transparency of operation.

#### **Key recommendations for privacy by design:**

- Organisations should be encouraged to implement high-level privacy management policies that will call for:
  - incorporating privacy impact assessments throughout the systems lifecycle from business case to decommissioning;
  - managing privacy-related risks to within pre-defined levels;
  - potentially submitting privacy impact assessments for the most sensitive systems to the ICO for verification; and
  - promoting greater transparency by publishing privacy impact assessments (this possibly being mandatory for public sector organisations).
- Organisations should be urged to demonstrate that all new systems support automated subject access requests, and encouraged to implement online subject access request services where appropriate.

## **Sharing personal information**

It is clear that data sharing is a commercial and government necessity, and any privacy by design approach must not only support the data sharing agenda, but also reduce the risk of failure and enhance the sharing outcome.

#### **Desired outcomes:**

- Organisations can share data internally and externally, and individuals have confidence that their privacy wishes will be respected when they do so.
- Individuals know who has their personal information and are able easily to access and amend it.

There is a clear need to develop a standard for data sharing that would allow organisations to incorporate secure and privacy-positive data interchange in their systems.

## Managing privacy metadata

Metadata languages have been researched for many years, but there are few examples of successful implementations for privacy purposes. Work is underway in the research community, including in the PrimeLife and EnCoRE<sup>23</sup> projects, to investigate the detailed requirements for policy languages to support metadata functionality and to encourage use and dissemination of standards through bodies such as W3C's Policy Languages Interest Group (PLING).

When personal information is shared from a system that is designed in a 'privacy-friendly' manner to another that is not, the privacy benefits may be lost. If metadata is stripped in the process (for example, if the receiving system is unable to process the metadata fields) then that personal information is left vulnerable to abuse.

Government, regulators, industry and academia should lend their support to the ongoing research work and seek out opportunities for innovative applications of the concepts that are developed. Whilst it is a long-term approach, the success of metadata is essential for the future of privacy by design.

## Information security standards for data sharing

A number of sector-specific regulators have issued guidance on the security controls that should be applied to personal information in transit, be it online or in physical media. For example, public authorities are mandated to encrypt personal information (which in most cases must also be protectively marked), and the Financial Services Authority is calling for similar controls in the finance sector.

These approaches should be extended across all organisations handling personal information. They will require clear and specific instructions about the circumstances under which they must encrypt data; the tools that they may use; and the processes that must be applied to managing the tools and associated encryption keys.

## Data minimisation

The most certain way to protect personal information during the data sharing process is not to share it – or even to hold it in the first place. This is the principle of 'data minimisation': that is, ensuring that systems collect, process and retain absolutely no more personal information than is necessary to meet the system objectives. Related issues, such as proportionality or necessity of processing, are equally important, and must also be taken into account in order to deliver a minimisation approach.

Data minimisation is largely a design philosophy rather than a technology solution, although specific technologies – such as privacy-friendly authentication mechanisms – can simplify the process.

Organisations need to be educated and reminded of data minimisation principles to encourage further use of this approach in future developments.

### Key recommendations for privacy by design:

- Government, regulators, industry and academia should reinvigorate research into standards for data sharing, including:
  - formalising approaches for collecting and managing privacy metadata;
  - developing PIA processes that can take into account the privacy implications of sharing data across many different systems; and
  - defining acceptable information security controls for the exchange of personal information.

The ICO will be in a position to guide and support this work.

- Future awareness initiatives from the ICO and other relevant regulators should restate and promote principles of data minimisation across all organisations.

<sup>23</sup> <http://www.encore-project.info/>

## Developing practical privacy standards

The lack of internationally recognised standards to guide organisations in implementing privacy controls, and differences between various local data protection laws at the international level, are an obstacle to achieving consistency in privacy management approaches across organisations.

### Desired outcomes:

- Organisations are able to operate in compliance with consistent, affordable, provable privacy standards, in much the way they already do with information security standards.

There are a number of initiatives under way to develop practical privacy standards. The need is great, as reflected by the adoption of a draft resolution 'on the urgent need for protecting privacy in a borderless world' at the 30th International Conference of Data Protection and Privacy Commissioners, on 17 October 2008.

Government, regulators, industry and academia need to come together to support this work and start preparing relevant standards in the UK, in partnership with emerging international activities. Ideally this work should come from end user organisations rather than regulators, since the outputs are then more likely to meet the wishes of the organisations concerned. Nevertheless, the ICO has an important role to play in catalysing and guiding such an approach.

### Key recommendations for privacy by design:

- Government, regulators, industry and academia should be encouraged to develop practical standards for privacy implementation, supported by guidelines for the functionality and specific technologies that should be considered for incorporation into new systems. This initiative has to come from the organisations themselves so that they contribute and collaborate to ensure that resultant standards meet their needs. The work should not be in isolation, but rather should engage with similar emerging initiatives elsewhere. The ICO has a role to play in guiding and supporting the initiative.

## Promoting privacy enhancing technologies

Despite many years of research, PETs have yet to find widespread adoption in 'real world' environments. Awareness and understanding of PETs is generally low, and even where PETs exist they often are not available in commercial products.

### Desired outcomes:

- Vendors are encouraged to incorporate PETs and privacy functions into their off-the-shelf systems and to promote these as selling points.
- Organisations adopt PETs into their systems where appropriate.
- PETs are recognised as valuable tools to support the management of personal information.

The key to delivering these outcomes will be turning important research in key PETs areas into deliverable products that vendors and enterprises can integrate into their systems.

### **Building a market for privacy products**

If the market for commercial products and systems that incorporate privacy functions is to grow, then major vendors need to see privacy as a key customer requirement – not just one of a number of functions, but a ‘deal breaker’ in any procurement. Until that happens, it is unlikely that they will be inspired to ensure that off-the-shelf products incorporate strong privacy controls. Government and private sector organisations should be encouraged to demand privacy functions as a core component of any software and system they procure.

### **Revocation and deletion of data**

A long-standing but still unresolved privacy management problem is that of giving individuals the ability to revoke already-given consent for the processing of personal information. Incorporating this need into systems is not always as simple as it seems: in environments where massive data sharing takes place, such as credit reference agencies or data brokers, if an individual’s record is deleted then it may rapidly be repopulated when data is imported from other sources. In such circumstances it may be necessary, and indeed legitimate, to hold a basic record of the individual so that it can be marked as a ‘desist’ and prevent further repopulation of the record.

The UK government is funding research into this area through projects such as EnCoRe, PVnets and VOME, and should support the development of commercial products based on the findings.

### **Privacy-aware authentication**

There appears to be a received wisdom within many organisations that when a system design requires an identification mechanism for individuals, then it is legitimate to ask ‘how much privacy shall be sacrificed to deliver identity?’ This attitude is at the heart of many flawed systems that inadvertently accumulate far more personal information than is actually required to deliver the desired objectives. Generally, an identification system has to be built around a database of personal information, whilst for an authentication system that is not necessarily required.

There is a need for much greater awareness of the identification and authentication mechanisms now commercially available to offer privacy-friendly services. Work by the likes of Credentica<sup>24</sup>, Liberty Alliance<sup>25</sup> and research projects such as PRIME<sup>26</sup> have developed practical commercial approaches to privacy-friendly identity mechanisms. Some of the most important work in this space has been done by Kim Cameron of Microsoft, who has developed the ‘Laws of Identity’<sup>27</sup>, which provide principles for privacy-friendly identification systems. These – and similar ideas – should be promoted to technology professionals involved in the design and delivery of any system that processes personal information.

### **Proving privacy by design**

Any approach that implements privacy by design will need to prove the effectiveness of that approach in order to satisfy consumers and regulators that the system or process really is privacy-friendly. For information security, this proof can be achieved using a combination of approaches that may include:

---

<sup>24</sup> <http://www.credentica.com/>

<sup>25</sup> <http://www.projectliberty.org/>

<sup>26</sup> Privacy and Identity Management for Europe (<https://www.prime-project.eu/>)

<sup>27</sup> <http://www.identityblog.com>

- assessing risks at a systemic level to confirm that the consequences of a breach are acceptable to the organisation;
- rigorous examination of the system design and implementation by accredited security professionals;
- testing of the implementation in simulated attacks ('white hat');
- opening up source code to public scrutiny; and
- obtaining independent certification of the level of security offered.

Privacy experts should prioritise further research into methodologies that can be used to test and prove privacy by design, and work with vendors to see how these can be delivered as practical products.

### Putting PETs into practice

The government, through its various innovation schemes in BERR and other agencies, is funding research into privacy issues. Such schemes should incorporate delivery of practical privacy products into their scope, and work with key vendors to ensure that the outputs are turned into commercial products.

Once practical PETs are available, there will be a need for an independent but trusted body – such as a regulator or trade association – which is able to test and accredit PETs-enabled products to confirm the level of protection offered and certify them accordingly. This is not dissimilar to the CAPS-approved function currently provided by CESG<sup>28</sup>.

#### Key recommendations for privacy by design:

- Government, regulators, industry and academia need to work together to support existing and future PETs research, and in particular encourage research into:
  - mechanisms to simplify obtaining and managing consent, revocation and minimisation;
  - 'privacy-friendly' identification and authentication systems; and
  - methodologies to test and prove the effectiveness of privacy controls in systems and across organisations.
- Successful initiatives should be developed into practical standards.

## Managing compliance and regulation

Perhaps the most important component of a privacy by design ecosystem is ensuring that every stakeholder complies with the agreed privacy requirements, and that an appropriate enforcement regime is available for those organisations that fail to do so. Only when this happens will individuals regain confidence in the responsibility and accountability of the organisations to whom they have to entrust their personal information.

#### Desired outcomes:

- Individuals know that organisations will be held to account for proper management of personal information.
- Organisations have a clear understanding of what information is considered to be personal and what powers individuals have over it.
- Privacy professionals are trained and accredited to known standards.

<sup>28</sup> [http://www.cesg.gov.uk/products\\_services/iacs/caps/index.shtml](http://www.cesg.gov.uk/products_services/iacs/caps/index.shtml)

## Ensuring accountability for personal information processing

It is clear that if any organisation is to be expected to take privacy needs seriously, then there needs to be both responsibility for privacy management (eg Chief Privacy Officer or equivalent), and possibly a concept of a 'nominated defendant' at executive level – a named individual who will be expected to represent the organisation in a criminal or civil court in the event of a data loss incident that results in legal proceedings.

An additional possibility would be to force organisations to declare an asset and liability value of personal information within their financial returns, thus forcing them to keep track of information assets and consider whether they are really required or not.

The topic of data breach notification – compelling organisations to inform regulators and individuals of data loss incidents – is very much in the spotlight at present, and may well provide a mechanism to improve transparency and accountability, but is not within the scope of this document.

## Empowering the regulator

If privacy by design is to succeed, then there is a role for an empowered and properly resourced ICO to encourage and enforce requirements. The ICO will require broader and clearly defined powers and bailiwicks with a mandate to govern:

- **behaviours:** including assigning accountability for proper data management;
- **regulations:** covering the UK and cross-border data transfers; and
- **outcomes:** including assigning and enforcing penalties and redress, and sponsoring class action lawsuits.

These powers and duties will need to be clearly communicated to data controllers and individuals alike. To achieve this, the ICO will also need the ability to recruit more technical experts who can communicate with developers, and support the current legal and management team. This has been the focus of the recent Ministry of Justice review, and the outcomes should be given whole-hearted support by the government.

## Clarifying legal complications

The private sector is seeking greater clarity on how to comply with the DPA and relevant European directives, since these prescribe the desired legal outcomes, but there are no recognised standards on how to achieve those. More efficient management of personal information (including emerging approaches that allow customers to manage their own information) would lead to a reduction in processing costs, more accurate and complete data, better consent processes, and ultimately a competitive advantage gained through responsible management of personal information.

There is a need to reiterate guidance across all affected stakeholder groups in order to build an improved climate of trust.

## Promoting the privacy profession

Organisations need to be able to recruit and retain individuals with accredited skills in privacy management. There is, as yet, no body in the UK that is widely recognised as providing such accreditation. ISEB<sup>29</sup> provides data protection qualifications, and the IAPP<sup>30</sup> is focused on the USA's requirements. There is, therefore, a clear need for a new professional body for privacy professionals in the UK.

---

<sup>29</sup> <http://tinyurl.com/64nn4y>

<sup>30</sup> <http://www.privacyassociation.org/>

Privacy professionals need to join together to develop a professional body that supports their profession through training and accreditation. It may prove to be more practical to do this – at least initially – under the aegis of another existing chartered body, with support from the ICO to ensure that all parties coalesce around a single organisation rather than multiple competing bodies.

This approach will create a new profession in which organisations can place their confidence, and which can deliver new privacy-related processes to support privacy by design. For example, qualified ‘privacy architects’ could sign off new systems to confirm the suitability of privacy controls, or accredit products to an assured standard. ‘Privacy auditors’ could even certify an organisation’s overall privacy practices as conforming to known standards, thus assuring individuals that their information will be handled in accordance with those standards.

#### **Key recommendations for privacy by design:**

- Regulators and government should explore the idea of obliging organisations to nominate an executive-level representative who will be held accountable for proper management of personal information.
- The government needs to recognise the realistic increased funding requirements of an empowered ICO that can both promote and enforce privacy practices.
- The ICO should examine whether there is a need for any further guidance on what constitutes personal information, and continue to deliver practical advice for organisations about what powers individuals have over their data.
- There is a pressing need for the development of a professional body for privacy practitioners (possibly under the aegis of an existing chartered body). The aim of this body will be to train, accredit and promote the work of privacy professionals. Clearly the ICO will have an important role in supporting this.

If you would like to contact us please call 08456 306060, or 01625 545745  
if you would prefer to call a national rate number.

e: [mail@ico.gsi.gov.uk](mailto:mail@ico.gsi.gov.uk)

w: [www.ico.gov.uk](http://www.ico.gov.uk)



November 2008

Information Commissioner's Office  
Wycliffe House, Water Lane  
Wilmslow, Cheshire SK9 5AF

ICO/PBD/1108/1K



Information Commissioner's Office