

March 2010

The Privacy Dividend: the business case for investing in proactive privacy protection

ico.

Information Commissioner's Office

The Privacy Dividend

ICO Overview

In 2008 the Information Commissioner's Office (ICO) commissioned a report on privacy by design which identified that an important barrier to proactive privacy protection was the absence of a soundly argued business case for investing in privacy friendly systems and business processes. It highlighted the lack of management engagement on the issue and concluded that organisations did not put an appropriate value on personal information; nor did they identify the potential cost of having poor privacy and data protection safeguards in place.

The ICO commissioned this report to help articulate the business case for investing in proactive privacy protection. It is intended to help organisations understand the business rationale for, and benefits to be gained from, building in better privacy protection. Its key conclusions are:

- personal information has a value and protecting it makes good business sense;
- it brings real and significant benefits that far outweigh the effort privacy protection requires;
- ignoring privacy and not protecting personal information has significant downsides.

The report analyses the value of personal information from different perspectives and outlines the consequences of privacy failures. It explains how to put a value on personal information and how to assess the benefits of protecting privacy. In doing this it does not stop at minimalist data protection compliance measures. It recognises that there is no 'one size fits all' approach and provides important practical tools in its appendices to help organisations construct customised business cases for investing in privacy protection. These include:

- guidance on the steps involved in a privacy protection scheme so organisations can assess costs and benefits of protecting privacy (Volume 2);
- guidance on creating business cases in two situations: implementing a new system or business process; and changing an existing system (Volume 2, Part 2);
- calculation sheets that organisations can use to assess the value of personal information and put numbers to the business case components. These include: valuation of personal information from four perspectives (Appendix C). privacy failure costs (Appendix E); and privacy protection benefits (Appendix F)

No organisation can neglect to think about protecting people's privacy when they are setting up new business systems and reviewing existing businesses processes. This report makes a valuable contribution to our efforts to encourage organisations to invest in proactive privacy and realise the 'Privacy Dividend'.

The Privacy Dividend

The business case for investing in proactive privacy protection

Volume 1 – The Business Case

Contents

In this document, Volume 1 - The Business Case:

The business case for executives	3
Introduction	5
The business case explained	6
Conclusion and recommendation	19
Authors' and Information Commissioner's remarks	20

In Volume 2 - Supporting Materials:

Part 1: Personal information in the business context	3
The privacy value of personal information	4
The consequences of privacy failures	13
The benefits of protecting privacy	19
The investment needed for the protection of privacy	23
Part 2: Creating the full business case	29
Part 3: Appendices	36
A: Glossary	37
B: References for Figure S1	38
C: Value of personal information calculation sheet	40
D: Worked example of harm to an individual	52
E: Privacy failure costs calculation sheet	54
F: Privacy protection benefits calculation sheet	58
G: Mandates for privacy protection	62

The business case for executives

- Protecting personal privacy makes good business sense.
- It should bring real and significant benefits that far outweigh the effort privacy protection requires.
- The alternative, of ignoring privacy and leaving personal information inadequately protected, has significant downsides.

Every organisation that processes personal information should set out to protect the informational privacy of every one of the people it affects. Not only is it the right thing for any responsible organisation to do, it also makes good business sense. Customers, citizens, employees and business partners will all trust the organisation more, and that will enhance the organisation's prospects for lasting success. Privacy failures could be very damaging to the organisation's reputation. Regulation requires privacy to be protected, and the strength of enforcement of privacy mandates is increasing.

An organisation that commits to respecting people's privacy and protecting their personal information will reap benefits. It will earn and deserve the trust of the people it relies upon and that will pay dividends in terms of those people's loyalty and their contribution to its success. It is more likely to have effective, well run information systems and processes. This will strengthen it operationally and improve its resilience. It will be operating with lower levels of risk, meaning it is less likely to violate someone's privacy and more likely to stay in control of its future. It will be able to have confidence in its compliance with legislation such as the Data Protection Act and with the privacy aspects of other regulations and mandates that bear upon it.

And the more committed and complete an organisation's approach to protecting privacy, the greater the rewards. Designing privacy in to the organisation's culture, and having privacy underpin every business information system and process, could enable the organisation to reduce both its operating costs and its risks at the same time as increasing its benefits – a triple win.

An organisation that does not respect people's privacy and does not protect their personal information would be selling itself and its stakeholders short. Any immediate gains to be had from taking privacy shortcuts will be superficial and short-lived; customers won will be just as easily lost, savings made today will be dwarfed by the costs of fixing the problems caused later. The organisation will be putting its compliance with regulations in jeopardy, risking fines and public censure.

And most importantly, it will not be able to stop privacy failures from occurring. Many of these will be minor but together they will erode the organisation's trustworthiness and reputation. And sooner or later one of these privacy failures will be serious. When that happens, everyone – customers, employees, business partners, regulators – will hear about it. The organisation's name and reputation will suffer, and the financial and operational impacts could be significant. If it is judged to have disregarded privacy or, worse, to have been careless, incompetent or negligent, it will be castigated. Its reputation will be damaged, the repercussions will be felt across everything the organisation does, and the effect will be long term disruption to the organisation's future prospects. In a really bad case, those accountable will be expected to lose their jobs.

For any organisation, its continued success depends upon it earning the trust of the public either as citizen, consumer or employee. Its success also depends on it earning the continued cooperation of third parties, such as business partners, suppliers and regulators. The public and third parties all base their trust and their attitudes towards the organisation on the organisation's reputation. In today's environment, reputation hinges increasingly on how the organisation treats its public and whether it meets their expectations, and this includes their privacy expectations. If an organisation builds privacy in to its information systems and processes, its reputation will be strengthened, the public's trust will be resilient, and it will improve its chances of long lasting success. If it ignores privacy and leaves personal information inadequately protected, it will be distrusted, continually having to chase short-term advantage, and hostage to the inevitable major privacy collapse.

Each organisation has to find its own course. Choose privacy protection and take the course that delivers the privacy dividend.

Introduction

In 2008, the Information Commissioner's Office (ICO) commissioned an expert report, entitled '[Privacy by Design](#)'¹. The purpose of this report was to identify why, more than 20 years after data protection legislation was first introduced into the UK, organisations have not done more to protect people's privacy. The report confirmed that there were still a number of barriers which needed to be overcome, including the need for a clear articulation of the business case for proactive privacy protection. It is in response to that finding that this report has been developed.

This report is in two volumes. The first makes that business case. It looks at why personal information should be protected and the benefits that organisations can expect to gain from protecting personal privacy. It concludes that protecting privacy should make good business sense for those organisations that process personal information regardless of their sector or size. The second volume provides a more complete discussion of each of the main components that make up that business case, and provides practical guidance and assistance to help organisations develop their own business cases tailored to their particular systems and circumstances.

This, the first volume, is aimed primarily at business leaders. As the reader will have seen, it opens with "The business case for executives" which states the unadorned business case plainly in a page and a half. The main body of this document is "The business case explained". Still aimed at business leaders, this explains the central ideas on which the business case is based. These are that personal information has value, that there are real and significant benefits organisations can gain from protecting personal privacy, and that privacy protection is a subject that needs board-level attention and leadership. This first volume closes with "Conclusion and recommendation" which invites the organisation's leaders to apply the conclusion from this work, that protecting privacy makes good business sense, to their own organisation.

The second volume is aimed at those senior personnel within organisations who are charged with putting the business case into practice within their organisation. In Part 1, it provides a more complete discussion of each of the main components of the business case. It explains how to put a value on personal information, and how to assess the benefits that the organisation might realise. It explains the consequences that can flow from privacy failures, and the costs and damage the organisation might expect to suffer from these. It then describes the main steps involved in a privacy protection programme so organisations can estimate the costs of protecting privacy within their information systems and processes, costs they will need to set against the benefits of protecting privacy.

Parts 2 and 3 of the second volume provide a wealth of practical guidance to practitioners. Part 2 recognises that different organisations will build their internal business cases in different ways, and explains how the materials covered thus far can be used or incorporated into internal business cases. Part 3 provides a range of calculation sheets and aides to help organisations put their own numbers to the business case components, plus other useful resources that support the earlier sections of the report.

¹ Privacy by Design, ICO, 28 November 2008, http://www.ico.gov.uk/upload/documents/pdb_report_html/privacy_by_design_report_v2.pdf

The business case explained

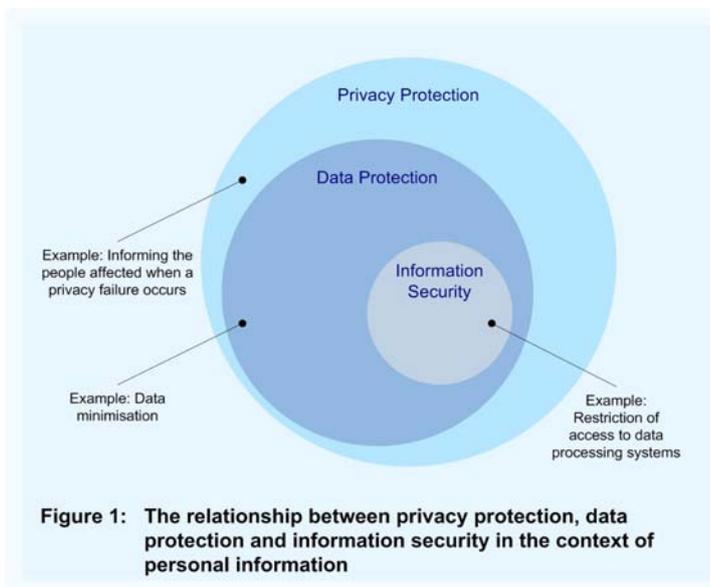
In this section we explain why protecting personal privacy makes good business sense. We describe what protecting personal privacy means, we explain why it matters, and we explain why this is a subject for Board-level attention.

Informational privacy

To start, we need to say how the term privacy is being used within this report. Privacy, in its fullest sense, is a combination of aspects such as physical privacy, spatial privacy, relational privacy and informational privacy. Here we are concerned only with informational privacy. By this we mean an individual's personal privacy as it might be affected by the attitudes and actions of others relating to the individual's personal information.

The protection of informational privacy is not solely about protecting personal information from being lost. Privacy failures can take many forms, including the gathering of excessive personal information and processing personal information unfairly. Protecting privacy involves the protection of people, either as individuals or collectively, from any type of harm or unwanted, unwarranted or unexpected interference that might occur as a result of the misuse or abuse of personal information.

What constitutes the acceptable use of personal information is a combination of what people themselves expect and the needs arising fairly out of the proper purposes of the organisation processing that information. People have legitimate expectations regarding how their personal information should be used and protected, and these should guide the way the organisation handles their information as much as the organisation's own view of its needs.



As this all indicates, the protection of privacy is not achieved solely by the security protection of personal information. For example, the protection of privacy requires ensuring that only necessary information is collected and that all information is accurate before it is used. Neither is it limited only to compliance with the Data Protection Act 1998 (DPA). For example, the wider protection of privacy might imply that people should be informed whenever they might have been affected by a privacy failure. Figure 1 illustrates this positioning.

Privacy is not contrary to efficiency, wealth creation, data sharing or Freedom of Information. It does, though, require that these aims be achieved in a manner that respects and incorporates the protection of privacy. This can be done by, for example, performing data sharing according to a

[privacy-protecting code of practice](#)², or recognising that providing a public or consumer good (e.g., convenience) is not sufficient on its own to justify unnecessary data capture or to presume the individual's consent.

Privacy is not an absolute goal and it does, in some situations, exist in a state of tension with other legitimate goals such as national security. However, the good of both the individual and society are often interrelated rather than simply antagonistic. In these cases, rather than privacy concerns being overridden roughshod, privacy concerns need to be weighed against other public goods. Judgement and a cautious approach is required so a person's privacy is not undermined unnecessarily or disproportionately in the pursuit of these other countervailing goals.

The privacy value of personal information

Privacy does matter and personal information does need to be protected. In this section, we explain the value of personal information from each of a number of perspectives, as it is this value that makes privacy matter.

Privacy value

The 'value' of an intangible entity such as personal information is an unclear term. Value for a tangible entity is normally thought of as the monetary worth of the entity, as measured by, say, the cost of creating it or the fair price that can be charged when selling it. This concept is difficult to apply to an intangible entity such as information in general. It is doubly difficult to apply to personal information, as none of the normal methods of determining an entity's value seems to capture well the importance personal information has to the individual concerned or the importance privacy has to society. However, these two are defining characteristics of personal information, and they are what makes the value of personal information much more than just the commodity value the information has to the organisation processing it.

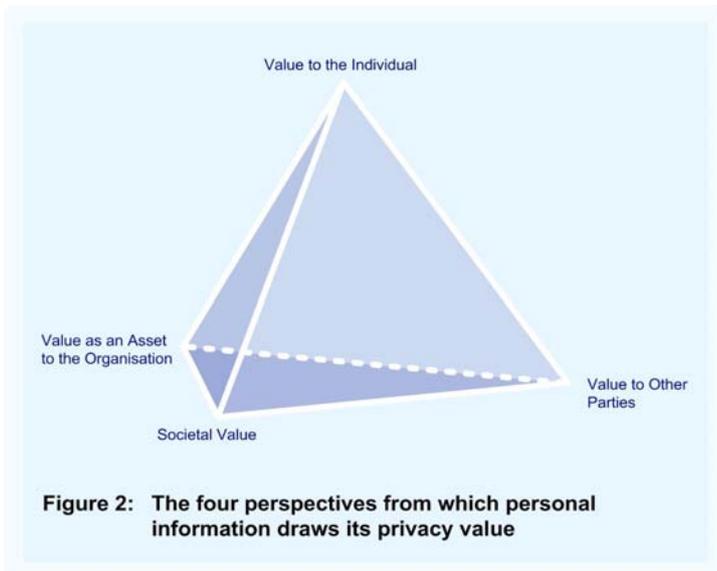
For any asset, 'value' is the intrinsic worth of the asset as seen from one or other perspective. It is what makes the asset worth protecting. It is what would be lost if the asset were not protected and it was then stolen or violated in some way. For personal information, the use of the term 'value' that is most appropriate to a privacy business case is as a measure of the importance of protecting the information in a way that protects people's privacy. Used in this way, 'value' reflects what would be lost if the information were unavailable or unusable, and the harms that could be caused to the individual and to society if privacy were violated.

As it is privacy threats and risks which are of concern in a privacy business case, 'value' is taken to mean the 'privacy value' of personal information.

² Framework Code of Practice for Sharing Personal Information, ICO, October 2007, http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/pinfo-framework.pdf

Four personal information perspectives

There are four perspectives from which personal information draws its privacy value. These are:



- its value as an asset used within the organisation's operations;
- its value to the individual to whom it relates;
- its value to other parties who might want to use the information, whether for legitimate or improper purposes;
- its societal value as interpreted by regulators and other groups.

We shall look at the privacy value of personal information from each of these perspectives in turn. We shall be focussing here on the value of personal information

where value is, as we have said, what makes the information worth protecting. It is important to distinguish value from other monetary measures which have a bearing on a business case. For example, value is not to be confused with the costs of protecting the information or the costs of dealing with a privacy failure should one occur. It is also not the same as the benefits that can be realised from the protection of the information. Both benefits and value are central to a business case, but they play different roles. We shall discuss value here and then focus on benefits in the next section.

1 - Value as an asset to the organisation

Personal information has value to an organisation when it is something the organisation exploits as it delivers its mission. The information might be information relating to customers, information relating to citizens, information relating to employees. It might be used for delivering goods, such as a person's contact details, for customising a product, such as personal preference information, or for controlling a service, such as entitlement information. Personal information can also have value to the organisation for more strategic purposes. It might, for example, be used to determine the opportunity value of a new service offering or for strategic decision making. Some uses will be common to many organisations and others will vary widely between organisations. The value each organisation places on personal information will, as a result, vary, and each organisation will need to determine that value for itself. This value can also vary according to the context in which the information is used, and it can change over time.

From this perspective, personal information is an asset for the organisation. As with any other asset, personal information needs to be protected to ensure it is used effectively within the organisation and its operational effectiveness and efficiency is maintained. Protecting it in ways which protects

people's privacy ensures that the additional asset value it has due to it being personal information is protected.

2 - Value to the individual

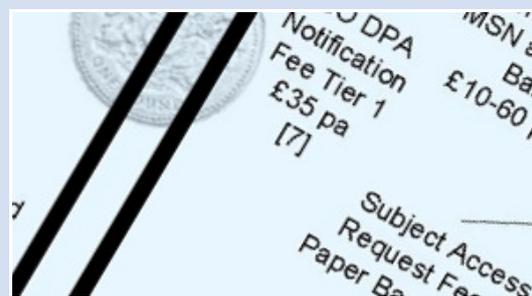
The second component to value comes from the importance personal information has for the individual to whom it relates. It reflects the fact that people could be harmed or caused distress if their personal information is used by the organisation in ways or for purposes other than those they expect or have agreed to (e.g., if it is used for profiling and they are unfairly denied a service or entitlement).

"Failure to respect an individual's privacy can lead to distress and in certain circumstances can cause that individual real damage, mentally, physically and financially."

What Price Privacy?³, ICO

When people provide their personal information, or agree to the organisation having their personal information, they generally expect the organisation to use it only for the accepted purposes and to handle their information carefully. This includes making sure that any third party the organisation passes their information on to also uses it and handles it carefully. These expectations are privacy expectations. They arise from the fact that if the organisation does not take care in the processing of people's personal information, people can be caused distress or harm. People expect that fair and reasonable organisations will not knowingly do things that would allow the people they rely upon to be harmed. Organisations need to acknowledge their capacity to affect people's lives inadvertently, and to assess how their current or intended information practices can, in any way, harm people or their interests, or impinge in any unwanted, unwarranted or unexpected way upon those people. It is this value component that makes protecting privacy at least as important as, rather than secondary to, protecting the asset value of the information as described above. Organisations need to take the importance the individual attaches to their information on board when determining the information's protection needs.

In Volume 2



In Volume 2, "Personal Information in the Business Context" extends this discussion on the value of information and presents a chart (Figure S1) of monetary values for various types of privacy-related data points

"...the public is showing high levels of concern over the potential mismanagement of their information. The two highest ranking concerns are security (96%) and passing or selling your details onto other organisations (95%)."

Annual Track 2008 – Individuals Report⁴, ICO

3 What Price Privacy? The Unlawful Trade in Confidential Personal Information, ICO, May 2006, http://www.ico.gov.uk/about_us/news_and_views/current_topics/what_price_privacy_now.aspx

4 Report on the Findings of the Information Commissioner's Office Annual Track 2008 - Individuals, ICO, December 2008, http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/ico_annual_tracking_individuals_final_report2008.pdf

Most people do value their privacy, though the extent to which they value it might not be clear, including to them, until the day their privacy is violated and the potential harm materialises. The person's age, background and general trust in organisations can all contribute to differences in the perception they hold of the value of their personal information.

From this perspective, holding and using people's personal information introduces significant risks for the organisation. If it is not careful how it handles people's personal information, and does not respect people's privacy concerns and expectations, the organisation can cause people distress or harm and that can rebound directly on the organisation, causing its reputation to be damaged. This risk is significant, and the organisation needs to take care with the personal information it holds to protect itself from this risk.

3 - Value to other parties

Personal information can also have considerable value to other parties. Some of these other parties might be those with legitimate purposes for using the information, such as those involved in the delivery of a requested service to an individual, and others might be parties that have wrongful or improper purposes in mind (e.g., criminals, competitors, disaffected employees, gossipmongers, hackers, investigation agencies, detractors such as hostile pressure groups and others out to discredit or damage the organisation).

Wrongful purposes might be malicious or criminal acts that cause harm to the individual, such as deception or fraud, or malicious or criminal acts that cause harm to the organisation, such as the theft of its customers or blackmail. Improper purposes might include unauthorised access to information by an intrusive employee, or purposes to which the individual concerned would clearly not have consented such as using information gathered for a benign purpose for covert monitoring and surveillance.

In Volume 2

Cost of acquiring or re-acquiring information method

Where this is not a market commodity, the amount of information that an organisation is willing to pay for is not the same as the amount of information that a person is willing to pay for.

Appendix C provides a calculation sheet to help the organisation determine the value of personal information in its own context

The value of personal information from this perspective arises from the fact that other parties, in their use of personal information, might cause harm or distress to the people concerned or damage to the organisation itself. This can arise if a legitimate purpose is undermined by the personal information being wrong, incomplete, insufficiently accurate, or simply not made available in good time. It can also arise if the other party, in using personal information for their own improper interests, causes harm through fraud or distress through embarrassment to the people concerned. In all such cases, damage

can also be caused to the organisation itself. These other parties are often external parties that the organisation has no direct influence or control over. However, the organisation is still accountable for maintaining the quality of the information it provides to legitimate parties and for keeping the personal information it handles out of the hands of other parties not authorised to have it. It is also important to recognise that these other parties can sometimes be under the organisation's influence or control,

such as a careless or errant employee or contractor. Then the organisation can most certainly be held directly accountable for their actions.

From this perspective, holding personal information introduces significant assurance-related risks for the organisation. As before, to prevent damage to its reputation and future prospects, and to protect possible damage and distress being caused to the people involved, the organisation needs to maintain the assurance of its personal information.

4 - Societal value

Privacy is not only about protecting the interests of individuals from harm. Privacy is, as is so often quoted, a right and a social value. The effects of the misuse or abuse of personal information bear not only at the level of the individual but also at the level of society.

“Privacy plays an important role in the social contract between citizen and state...”
A Surveillance Society?⁵, House of Commons Home Affairs Committee

This societal value places an imperative on the organisation to protect people’s privacy, and it takes two forms. The first way it manifests itself is most organisations’ desire, in many cases their strong desire, to “do the right thing” with regard to privacy, i.e. to be trustworthy, transparent, and respectful of people’s privacy. Where this exists, it forms a major component of the culture of the organisation and of the reputation the organisation projects to its public. It has a powerful influence on the confidence, trust and loyalty people feel. This then has a direct bearing on the organisation’s prospects, its ability to be effective in what it does, and its ability to implement strategic change successfully when it needs to.

“... privacy is in itself a value that needs protecting, even when the loss suffered is not readily quantifiable in terms of damage or distress.”
What Price Privacy?⁶, ICO

The second form this component of value takes is the value given to the protection of privacy by regulators. Regulators act on behalf of groups of individuals, sectors, or society as a whole. They ensure that the interests of individuals (e.g., their right to be treated fairly), interests external to the organisation itself (e.g., market efficiencies), and interests beyond those of any one individual (e.g., democratic freedoms), are suitably protected. They may also address those situations where the effort or expense if an organisation were to address the problem is lower than the cumulative effort or costs if it were left to individuals individually to address the problem. Where one individual can have only a limited effect on an errant organisation, for example withdrawing their support or taking their custom elsewhere, regulators and legislators have the means to amplify the power of the individual to the scale of the population or society as a whole.

5 A Surveillance Society?, House of Commons Home Affairs Committee, The Stationery Office Limited, 8 June 2008, <http://www.publications.parliament.uk/pa/cm200708/cmselect/cmhaff/58/58i.pdf>

6 What Price Privacy? The Unlawful Trade in Confidential Personal Information, ICO, May 2006, http://www.ico.gov.uk/about_us/news_and_views/current_topics/what_price_privacy_now.aspx

External mandates include legislation such as the EU directive 95/46/EC⁷, the DPA in the UK, stronger, equivalent or alternative privacy legislation in other countries, and other-country legislation with overlapping interests (e.g., SOX⁸ and GLB⁹ in the US). In addition, increasing numbers of UK

In Volume 2



Appendix G provides a worksheet to record mandates and also highlights some UK regulators, trade organisations and associations that mandate privacy protection

sectoral regulators and trade bodies are putting their weight behind DPA requirements and sometimes impose additional requirements of their own.

From this perspective, in its two manifestations (the organisation's concern to "do the right thing" and the concerns expressed by regulators and legislators), the societal value of personal information places an imperative on the organisation to protect privacy. It enlarges the risks that holding personal information introduces to the organisation and doubles the need for the organisation to protect people's privacy.

The benefits of protecting privacy

The preceding discussion explained the different sources for the value of personal information. In so doing, it established the rationale for protecting privacy. It explained why personal information needs to be handled carefully and to be protected. By protecting privacy, small, medium and large organisations can also reap real and significant benefits – the privacy dividend. Here we explain what these benefits could be.

Protecting people's privacy can bring substantial benefits to the organisation. These are real benefits in that they help the organisation to succeed and to achieve its business objectives. Some of these benefits are mission-enhancing benefits, such as increased take up of services, revenue up-lifts or cost reductions. Others are risk-reducing benefits, such as improvements in resilience or the reduction of assurance or compliance risks.

To show how these benefits might arise, we shall again invoke the four perspectives introduced above from which personal information acquires value. Where value provides the rationale for protecting privacy, the benefits provide the motivation. These benefits will carry different weights for different organisations, and each organisation will need to determine for itself how much incentive each benefit provides¹⁰. Together for any one organisation, these benefits form the foundation on which the business case for protecting people's privacy is made.

7 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281 , 23/11/1995 P. 0031 - 0050, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML>

8 Sarbanes-Oxley Act, or Public Company Accounting Reform and Investor Protection Act

9 Gramm-Leach-Bliley Act, or Financial Services Modernization Act

10 In Volume 2 of this report, we provide a number of tools to help organisations assess these benefits.

1 - Benefits from protecting the value of the information as an asset to the organisation

Protecting personal information as an asset helps to make the organisation's operations efficient and productive, agile in the face of change and new opportunity, and attractive to its public. It helps to keep operating costs down by, for example, avoiding the organisation having to collect the same information repeatedly or hold multiple copies of the same data. It helps to increase returns because the people being served benefit themselves from having their personal information being kept correct, accurate, complete and available. Doing this enhances the organisation's reputation, makes its offerings more attractive, and enables the organisation to respond more rapidly to people's requests. And it helps to protect the organisation against operating risk by, for example, helping the organisation to avoid providing a person with the wrong service or not being able to provide them with the right service at the right time. It also helps to ensure that any strategic decisions made based on personal information will be sound and well balanced.

2 - Benefits from protecting the value of the information to the individual

Respecting people's privacy and responding to people's sensitivities and concerns earns the organisation people's trust and confidence. This can provide an uplift in that the organisation's reputation will be enhanced and people might be more willing to support the organisation and take up its services or offerings. The commercial value of enhanced trust is recognised, with evidence showing that stronger trust can lead to an increase in profit margin¹¹. Trust can, and should be, seen as a positive contributor to business success. Where the people are employees, if they believe the organisation is trustworthy they might feel more of an imperative to be trustworthy themselves in their dealings with the organisation, and more able to show initiative, creativity or enthusiasm on behalf of the organisation. As a result, enhanced trust could help the organisation to be effective in what it does and be successful at implementing necessary change when it needs to.

Respecting privacy can also help to keep the organisation's operating costs down¹² by, for example, people being willing to provide additional or truer information as an alternative to withholding information or providing false information. And, as importantly, people's trust makes their loyalty more long-lasting and resilient. No organisation can meet everyone's expectations in full all the time. If it earns their trust, people are more likely to remain loyal despite the occasional 'bump in the road'. If it fails to earn their trust, people might leave without notice and without bothering to give the organisation a chance to address their complaints.

From this perspective, respecting and protecting people's privacy is one part of respecting them as people for the value they bring to the organisation. Whether that is the value they bring as paying

In Volume 2



"The Consequences of Privacy Failures" and Appendix E, in Volume 2, discuss the forms of damage that could affect the organisation and provide a calculation sheet to identify the potential costs

¹¹ Resnick, P. (2006) The value of reputation on eBay: a controlled experiment. *Experimental Economics*, volume 9, Issue 2, Jun 2006, Page 79-101

¹² Willcocks, L. P., and Cullen, S. (2006) *The Outsourcing Enterprise: The Power of Relationships*

customers, as users of the services the organisation provides, or as employees working hard on the organisation's behalf, respecting their privacy is the fair return the organisation gives them for the value they bring. If the organisation fails to provide that return, it could lose their loyalty and shortly thereafter lose their value.

One further benefit to protecting privacy is that the organisation can avoid or reduce the costs associated with inadvertently violating people's privacy. Failing to protect people's privacy exposes the organisation to the risk of, for example, using information which is inaccurate or using it without consent. Where this causes people harm or distress, the organisation will then be faced with the direct and indirect costs associated with that privacy violation. These can include the costs of fixing the processing or procedural fault that led to the privacy violation, the costs of compensating the people affected for any losses they might have suffered, and any harm caused to the organisation's reputation. Though these costs are associated with not protecting privacy adequately, the reduction of these costs can be seen as a benefit flowing from privacy protection.

3 - Benefits from protecting the information from other parties

Protecting personal information from these, mainly assurance-related, risks should reduce the chances of the organisation damaging its relationships with its public and losing the investment it has made in those relationships. Though the threats from which personal information is being protected under this perspective are different from the threats relating to the preceding perspective, some of the benefits of protecting the information are quite similar. The similar benefits are those that come with an enhanced reputation and strengthened relationships. Less similar are the benefits associated with reducing the risk of privacy failures. The impact and costs on the organisation of allowing another party to misuse and abuse people's personal information can be more serious than those associated with the organisation misusing the information itself. The harm caused to the people affected can be more serious and, as a result, the costs associated with the privacy failure more substantial.

Another benefit unique to this perspective is that protecting personal information could help to protect the organisation from competitive disadvantage. This can be the case, for example, if the information is obtained by a competitor and could be used by them to gain a competitive lead, or could be used by someone hostile to the organisation to cause it embarrassment through its disclosure.

4 - Benefits from protecting the societal value of personal information

From this perspective, personal information needs to be protected for two reasons: because the organisation believes it is important to "do the right thing" with regard to privacy, and to improve compliance with applicable external mandates.

"Doing the right thing", i.e. projecting attitudes and behaviours regarding personal privacy that are deemed fitting by its public, increases the confidence, trust and loyalty these people feel in the organisation. This attracts the positive benefits and reduces the costs associated with privacy violations as already discussed above. Where the organisation has a public brand (locally, nationally or internationally), not only could the one organisation's reputation be lifted by "doing the right thing" but the reputation of the sector or community to which it belongs could also be lifted. This provides benefits to all member organisations. In the case of groups of organisations working together, it is possible that this might reduce the likelihood of future additional legislation and greater compliance

costs¹³. Enhanced public trust in a sector could lift that sector's market size. Enhanced public trust in one central government department could encourage citizen engagement with all departments.

The impact of being found non-compliant with external privacy mandates could be large^{14 15 16}, meaning that the benefits of improved compliance can be correspondingly large. Compliance with multiple mandates is complex, especially where many geographic locations are involved, and the penalties for non-compliance range from private censure through fines and penalties to restrictions on operating licences that can put future opportunities and operations at risk. Any significant compliance shortfall can also bring public censure and associated reputational damage which impairs future prospects. The legal costs, plus the need to address the root cause of non-compliance in a manner and timeframe not of the organisation's choosing, can also prove very expensive.

The absence of prescriptive measures within most mandates introduces the risk of misinterpretation of a mandate's requirements and unintentional non-compliance. For example, this was cited as a contributory reason for the MoD's major data breach of January 2008¹⁷. Taking a positive approach to privacy protection that aims to exceed the minimum requirements by a clear margin would provide a significant benefit by reducing this compliance risk.

As technology advances and organisations' infrastructures become more complex, information transparency becomes ever more difficult. It becomes increasingly difficult for people to discover what happens to their personal information, who handles it, when and for what purpose. As a result, society's reliance on transparency and accountability by organisations will only increase as technology advances, not diminish. It is to be expected that the penalties for non-compliance with privacy mandates will increase over time too. There is a clear trend in this direction already discernible^{18 19 20}. Hence, the magnitude of the benefits from maintaining high standards of privacy compliance are likely only to grow.

Taking a positive approach

The value of personal information establishes the rationale for protecting privacy. The many possible benefits provide the motivation. Here we argue for organisations to embrace privacy fully and to do more than just the minimum necessary to avoid failure.

Organisations have options regarding the approach they take to protecting privacy. Those that are sceptical of the benefits and focussed primarily on the implementation costs privacy protection might

13 Can We Keep Our Hands Off The Net? Report of an Inquiry by the All Party Parliamentary Communications Group, October 2009, http://www.apcomms.org.uk/uploads/apComms_Final_Report.pdf

14 Press Releases, ICO http://www.ico.gov.uk/about_us/news_and_views/press_releases.aspx

15 Press Releases, Financial Services Authority 2007-2010, <http://www.fsa.gov.uk/Pages/Library/Communication/PR/>

16 Adjudications, PhonepayPlus, <http://www.phonepayplus.org.uk/output/Adjudications.aspx>

17 Report into the Loss of MOD Personal Data, Sir Edmund Burton, Ministry of Defence, 30 April 2008, http://www.mod.uk/nr/rdonlyres/3e756d20-e762-4fc1-bab0-08c68fdc2383/0/burton_review_rpt20080430.pdf

18 Knowing or Reckless Misuse of Personal Data - Introducing Custodial Sentences, Consultation, Ministry of Justice, 15 October 2009, <http://www.justice.gov.uk/consultations/misuse-personal-data.htm>

19 Civil Monetary Penalties - Setting the Maximum Penalty, Ministry of Justice, 9 November 2009, <http://www.justice.gov.uk/consultations/civil-monetary-penalties-consultation.htm>

20 Information Commissioner's Guidance About The Issue of Monetary Penalties Prepared and Issued Under Section 55C (1) of the Data Protection Act 1998, ICO, 12 January 2010, http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_guidance_monetary_penalties.pdf

entail, might be inclined to adopt a minimalist approach, doing no more than is necessary to avoid failure so they can limit their implementation costs. This could be a false economy. Taking a more resolute approach to protecting privacy could increase the magnitude of the benefits well beyond any increase in costs. This approach is sometimes referred to as “privacy by design”²¹.

In the context of the business case, there are three components to a ‘privacy by design’ approach and each helps to amplify the benefits achievable.

Proactive rather than reactive

Lead rather than be led. Privacy should be designed into an information system or process as soon as possible, and for a new system or process, from the first stages of design. As with any other aspect of design, it is widely recognised that it is easier, faster and normally cheaper to get the design right first time than to have to make corrective, possibly more complex, changes later on in the system’s lifetime, or at very short notice. Being proactive with either new or existing systems and processes should also reduce the opportunity for public censure and fines.

Comprehensive rather than minimalist

The Data Protection Act (DPA) is the minimum requirement for privacy protection not the maximum. And, as it clearly cannot be prescriptive and specify the specific measures an organisation must apply, taking a minimalist approach risks the organisation falling short and perhaps unintentionally breaching the DPA. A comprehensive rather than minimalist approach reduces this risk. It also increases the scope for achieving benefits. The more comprehensive the level of privacy provided by the organisation, the greater the differentiation between the organisation and its peers or competitors, the greater its opportunity to introduce efficiencies, and the greater the level of control it has.

Taking a comprehensive approach also reduces the whole-life costs for each system. A minimalist approach does not remove the risk of privacy failures occurring. Over the lifetime of the system or process, failures will still occur and each will require a fix to be implemented. Thinking comprehensively is likely to be less costly than continually having to implement individual unplanned privacy measures in response to critical audits or actual privacy failures.

Enterprise-wide rather than case-by-case

Firstly, larger organisations, and certainly international organisations, tend to find they have a multitude of different privacy mandates with which they need to comply. An enterprise-wide approach that address all mandates under one framework is almost certain to reduce the effort and cost associated with achieving compliance with multiple sets of requirements.

Secondly, protecting privacy is closely intertwined with managing information properly. Taking an enterprise-wide approach to privacy protection should encourage and facilitate stronger management of personal information. This would attract a number of benefits normally associated with better information management:

21 A term developed by Ann Cavoukian PhD, Information and Privacy Commissioner of Ontario, Canada

- Reduced wastage and risk collecting, storing, maintaining and protecting personal information that is not productive.
- Better positioning to enter new markets and to respond to changing markets.
- Better positioning to take advantage of new technological approaches.

“61% of private organisations now believe that the DPA adds value to their business, and 83% believe that it improves customers’ trust – these are critical messages for a commercial operation.”
[77% and 92% respectively for public organisations]

Annual Track 2008 – Organisations Report²², ICO

Protecting privacy by design can be applied to existing information systems and processes as much as to new ones under development²³. An information system may have managed to avoid being the cause of a privacy failure in the past but that does not mean it will not be the cause of one in the future. And public trust, once lost can be very difficult and costly to recover. Hence, it is never too late to consider implementing privacy protection within an existing information system unless it has reached the end of its life and is being decommissioned.

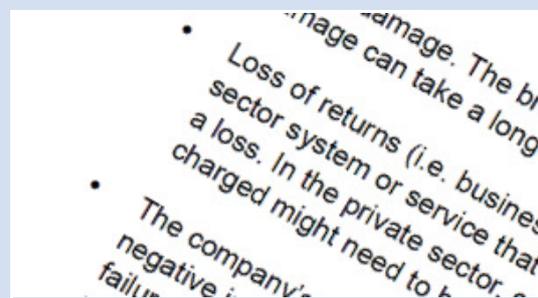
The need for the Board’s engagement

As has been explained, the value of personal information makes it important that all organisations handling personal information protect the privacy of the people whose information they hold. In addition, the benefits of protecting privacy should contribute significantly to the success of an organisation, and the impact of not protecting privacy adequately could impair the organisation’s prospects. For these reasons, privacy protection needs to be given a high priority within every organisation and to be under the direct control of the Board. It is too closely linked to the success of the organisation to be left to technical or middle management who might not recognise the breadth of its impact on the organisation and might see only the narrower benefits of, or costs to, the business area, project or role they are engaged in.

Accountability for something as important as privacy protection and the protection of the organisation’s reputation rightly belongs with the Board. In addition, there are a number of other reasons why privacy protection should be under board-level control.

- Privacy protection is not a project with a start and an end, it is an attitude and approach that needs to be woven into the culture of the organisation and from there

In Volume 2



Volume 2 provides further information about assessing and implementing proactive privacy protection with practical steps and additional guidance

²² Report on the Findings of the Information Commissioner’s Office Annual Track 2008 - Organisations, ICO, December 2008, http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/ico_annual_tracking_orgs_final_report2008.pdf

²³ Privacy By Design resources, ICO, http://www.ico.gov.uk/about_us/news_and_views/current_topics/privacy_by_design.aspx

to inform and guide all the 'business as usual' activities employees perform on or with personal information. Cultural leadership cannot be driven from anywhere other than the Board.

- Privacy protection measures can be organisational and procedural as well as technical. Many functions (for example, Legal, Operations, Information Systems, Public Affairs, Marketing) will need to bring their privacy measures into line to ensure that the organisation's response is consistent and efficient and serves the organisation's enterprise-wide goals and strategies. This can be driven only by the Board.
- In addition, there might be organisational, cultural or strategic barriers that will need to be overcome, and to remove these barriers will need the authority of the Board.
- Initial funding to get a privacy improvement programme under way should be made available by Board sanction so it is protected. In difficult economic times, all funding comes under pressure. Yet it is in difficult times that the benefits of a strong stance on privacy can be all the more important, giving the organisation greater resilience to periods of hardship.
- As privacy within the organisation matures from being an improvement initiative to becoming a core aspect of business as usual, commitment to the protection of privacy will need to be reinforced continually across the organisation by the visible demonstration that privacy protection remains important to the wellbeing and success of the organisation. Maintaining this focus over the long term will need the vision that is held by the Board.

The Board's direction is needed so that employees appreciate that all parts of the organisation need to be involved in a privacy improvement programme. Every function head will need to support the programme and identify how improving privacy protection aligns with their mission, business objectives and goals. Non-Executive Directors and other advisors will serve to deepen the organisation's understanding of the different approaches and strategies available and to help identify which approaches will be most appropriate and successful. All executive and senior management will need to be involved personally in weaving privacy awareness into the culture of the organisation and demonstrating through the positions they adopt the priority that is to be given to privacy protection.

Conclusion and recommendation

This document has presented the business case for the protection of personal privacy. The case has been made on the basis of the value of personal information and the benefits organisations can reap from its protection. Personal information has real value. Its protection provides meaningful benefits, and inadequate protection could lead to significant losses in many forms.

The conclusion reached is that the business case for protecting privacy is a positive business case. The recommendation is, therefore, that each organisation should take this business case on board and make sure that it protects the privacy of the people on which it relies.

The challenge each organisation faces is to specify for itself the business case that exists for strengthening its approach to privacy and improving the way it protects personal information. Some organisations will have to take on more change than others, or will have a greater number of opportunities to gain benefits than others. Some organisations will want to take privacy protection somewhat further than others. Each will have to set its own privacy goals and set its own timeframes for achieving those goals.

To meet this challenge, each organisation will need to go through the process of determining the value of the personal information it processes, the benefits it can expect to reap, the implementation costs it can expect to face, and to develop a business justification tailored to its own particular circumstances. This will not be an easy task. However, it is a highly important task. We believe it can be achieved and to that end hope that the materials provided in this and the supporting document will provide the necessary assistance.

Authors' remarks

When speaking with organisations that have implemented privacy protection, they told us without exception that there are many benefits to protecting privacy beyond just compliance with the DPA. Our two documents share their knowledge and experience so that all types of organisation, public and private, large and small, can benefit from their experience and leadership. These documents do not provide a treatise on privacy protection, nor do they present novel research findings. They simply forge from the large volume of available material a business case for privacy protection in a form we hope is clear, direct and compelling.

We wish to express our gratitude to the many organisations and individuals who have, by sharing their time and their views, contributed to this work.

John Leach
John Leach Information Security Ltd
3rd March 2010

Colin Watson
Watson Hall Ltd
3rd March 2010

Information Commissioner's remarks

Increasing amounts of personal information is now held about us as part of everyday life. Even though we have had data protection laws for 25 years, continuing privacy incidents, such as with well publicised data losses, show that more still needs to be done to help ensure that personal information is properly protected. Protection cannot be left to chance or be seen as doing only the bare minimum necessary to comply with the law; proper safeguards have to be built in from first principles, not bolted on inadequately as an afterthought.

Our previous research into 'Privacy by Design' identified a number of areas where more could be done to ensure adequate privacy safeguards are designed in to the systems that handle personal information. One important deficiency identified in that research was the absence of a well argued business case for investing in proactive privacy protection. As a result, we commissioned this report to provide that rationale.

This report has risen to that challenge. It analyses the value of personal information in different contexts and the consequences of privacy failures. It also recognises that there is no 'one size fits all' approach and provides important practical tools in its appendices to help organisations of any size or sector construct custom business cases for investing in proactive privacy protection and realising the 'Privacy Dividend'.

Christopher Graham
3rd March 2010

The Privacy Dividend

The business case for investing in proactive privacy protection

Volume 2 – Supporting Materials

Contents

The main document presents the business case for proactive privacy protection plus recommendations. This supporting document contains discussion and a number of materials to help organisations tailor that business case to their organisation.

Part 1: Personal information in the business context	3
The privacy value of personal information	4
The consequences of privacy failures	13
The benefits of protecting privacy	19
The investment needed for the protection of privacy	23
Part 2: Creating the full business case	29
Part 3: Appendices	36
A: Glossary	37
B: References for Figure S1	38
C: Value of personal information calculation sheet	40
D: Worked example of harm to an individual	52
E: Privacy failure costs calculation sheet	54
F: Privacy protection benefits calculation sheet	58
G: Mandates for privacy protection	62

This document

Part 1 covers the material discussed in the main document in greater depth to help organisations identify the value of personal information from their perspective and the benefits they should expect to achieve. It also covers the impacts that privacy failures could cause, and the investment that might be associated with a privacy improvement programme.

Part 2 describes how the material discussed can be used to build a typical business case for a specific programme or project.

Part 3 provides the other materials referenced by the main business case and elsewhere within this supporting document. These include various useful references and calculation sheets to help organisations develop their own numbers, and supporting materials for the business cases they might need to make.

Part 1: Personal information in the business context

In the main document we explained the business case for protecting personal privacy. Here we discuss in greater detail the central concepts on which that business case was built, to help organisations in their preparation of tailored business cases for their organisation.

Approach

The value of personal information has been shown to be a combination of different value components. Likewise, the overall benefit to the organisation protecting privacy is the combination of a number of different benefit components.

The weight each of these components carries will vary from organisation to organisation. This is to be expected. For example, the cost of customer acquisition and the expected return per customer will be different in a bank between a high-net-worth individual and a typical retail customer. They will vary from one bank to another, and they will vary from a bank to an energy supplier to a solicitor's practice. Similarly, the ways in which organisations would set out to protect privacy, the measures they would apply and the costs they would incur, will all vary from organisation to organisation. Every component within a privacy business case will be organisation-specific.

As a result, each organisation has to determine for itself what weight or numerical values are right for it to assign to each of the components it uses within its business case. Here we look at each of the components that should have a bearing within a privacy business case, to give organisations a hand in determining their weights and values.

The scope of 'personal information'

Personal information includes any information that relates to a particular person, whether shared or unique. It is not limited to information that identifies a person directly (sometimes referred to as personally identifiable information - PII) and it is not limited to only the more sensitive items of a person's information such as their medical or ethnic details. Given the power of contemporary search and aggregation tools, non-identifying information could be used in combination with other non-identifying information to identify a person to a high level of confidence. That a person lives on a particular road in a particular village, their gender, the decade in which they were born, their marital status, the type of car they drive and whether they commute a long way to work every day, none of these is unique to that person or is, on its own, particularly sensitive. However, together they can lead to the identification of an individual and could, for example, enable a burglar to assess whether they might be a good target during work time.

Hence, each person will have concerns about the use and protection of any piece of their personal information, whether sensitive on its own or not. Organisations need to treat all the personal information they handle as requiring privacy protection.

The privacy value of personal information

The general business case explained that personal information has value, privacy value, and that, for a variety of reasons, any organisation processing personal information should protect the privacy of the people to whom that information relates. Here we expand upon that discussion to help organisations understand how that value arises. Later within this supporting document, we provide a calculation sheet to help organisations determine the privacy value of the personal information they process.

Gauging the value of personal information

As explained in the main document, personal information has value according to each of four different perspectives. Value is a measure of the importance that the information is protected. This importance comes from the duty of protection placed on the organisation (for example, the duty to stakeholders to protect an asset, the duty to individuals to protect them from harm, the duty to society to protect societal values) and it comes from the magnitude of the damage that could be caused (to the organisation or its stakeholders, to the individuals, to society) if that information is not adequately protected.

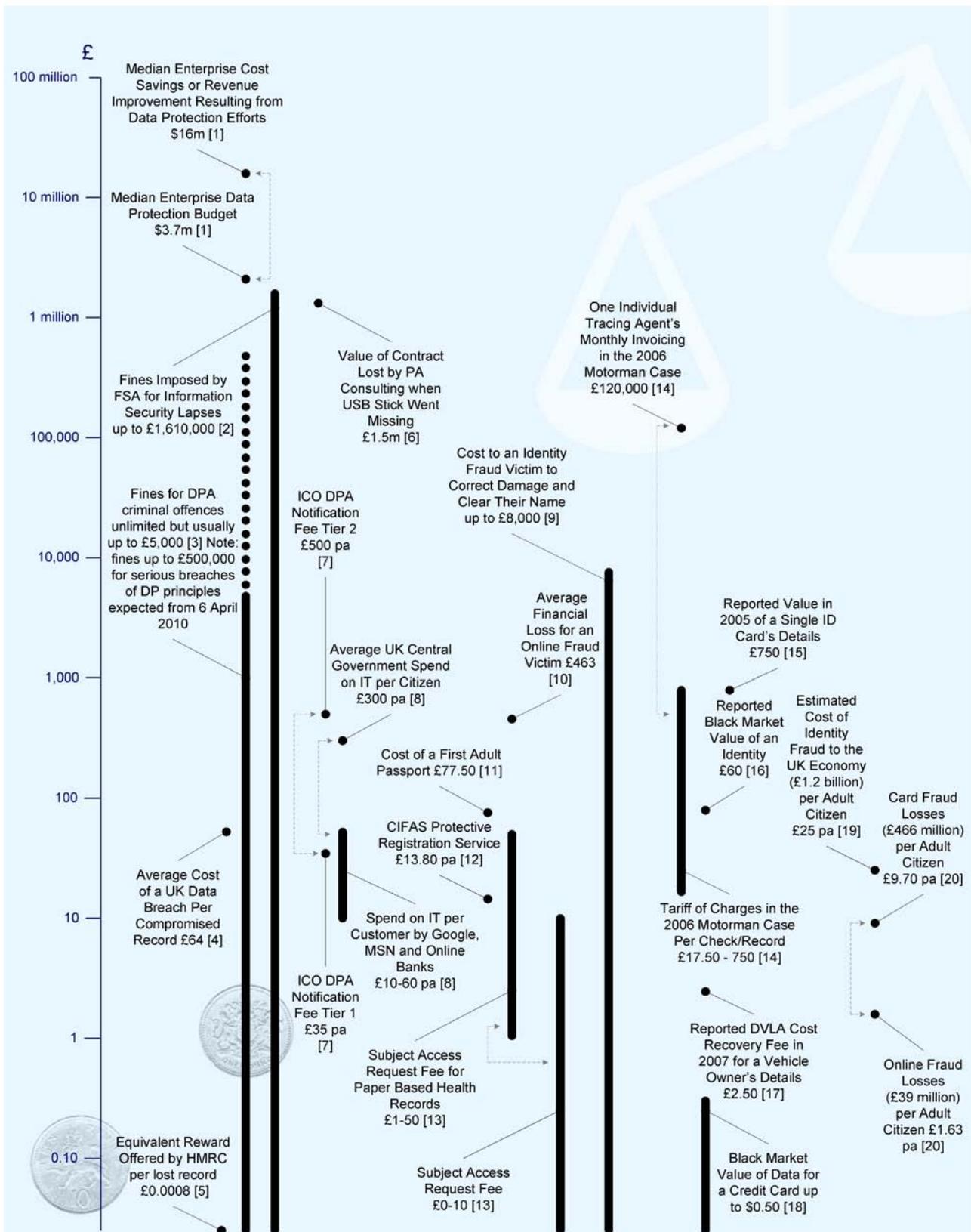
Value may not always lend itself to being quantified well in financial units, and even when it does, the financial value determined by one organisation may be different from that determined by another¹. Regardless of this, organisations will probably need to determine a value result for the personal information they process as input to their business cases. In these cases, they will need to identify the personal information they hold and then gauge the value of that personal information from each of the four perspectives using whichever method is best suited to the nature of their business processes. The overall value, i.e. the overall need for privacy protection, will be determined by the largest of the values this process identifies.

The chart in Figure S1 on the following page illustrates, on a logarithmic scale, monetary values for various types of privacy-related data points. Most data are plotted on a per person or per event basis, but some are shown per month or per annum. These figures are purely illustrative and should not be used as more than that. They show a wide variation between values, especially when those have been calculated as averages for large numbers of records. We shall refer to this chart several times as we discuss valuing personal information below.

1 – Value as an asset to the organisation

Personal information is used within some, possibly many, of the organisation's operational systems and processes, and for some organisations it might even be the lifeblood of the business. Clearly, in these cases, personal information is an asset much as is any other essential component, tangible (such as a piece of machinery) or intangible (such as a trade secret). And further, not only is personal information an asset, the trust gained when that personal information is well managed and protected is also an asset. They both require investment and maintenance, and deliver continued value over time. They might not feature on a balance sheet but that does not mean they are not of concern to an organisation's leaders or the organisation's stakeholders.

¹ Value of Information Subgroup, EURIM, <http://www.eurim.org.uk/activities/ig/voi/voi.php>



If the value of personal information as an asset is not appreciated, it is likely the information will not be managed well, it will not be exploited fully, which would be wasteful, and value and trust could be eroded without the organisation fully appreciating what it is losing.

From this perspective, an organisation could gauge the value of the information in any of a number of ways. It could be gauged by considering variously,

- the cost of re-acquiring quality information,
- the amount of business or mission which depends on the information,
- the cost to the organisation if the information cannot be used and information-based processes are impaired,
- the value of the resources being used to store, process, maintain and protect it,
- the impact if the organisation has to fall back on more costly alternative processes.

Or it could be valued using whatever particular approach the organisation takes for other of its intangible assets if that would seem appropriate. In strategic or management decision making, the value of the information is related to the opportunity value the information supports.

The calculation sheet available as Appendix C within this document can help organisations to determine the asset value figures that are right for their operations and processes.

2 – Value to the individual

Despite it being commonly stated that people do not value privacy in these days of social networking, studies that have tried to understand people's attitudes tend to confirm that most people do still value their privacy. Some people value it more than others, some value it very highly and others value it hardly at all. The studies show that where people do value it, they have firm expectations regarding how their personal information should be used and that they should be able to give and revoke meaningful consent.

Awareness of the importance of privacy appears to be growing². People are becoming increasingly sensitive about the capture of their personal information as they become more aware of the everyday use of information systems. They understand that whilst the proper use of their information can be beneficial to them, its improper use by the same organisation can cause them harm. They understand that this type of misuse is not necessarily infrequent, whether due to human carelessness or procedural error. And they understand that they can be harmed even when their personal information is used within a system or business process as intended, owing to the presence of system design weaknesses that could lead to privacy failures.

Organisations that processes personal information should acknowledge that they have the ability, whether by design or otherwise, to cause people distress and harm. This places a duty on each organisation to consider, based on the information they hold and the processing they regularly or might perform, how people might be affected by possible privacy failures, accidental or otherwise.

² Report on the Findings of the Information Commissioner's Office Annual Track 2008 - Individuals, ICO, December 2008, http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/ico_annual_tracking_individuals_final_report2008.pdf

The value of personal information under this perspective is set by the magnitude of the harm and/or distress people might suffer as a result of such a privacy failure. The harm and distress caused is the harm and distress as experienced or perceived by the people affected. It is people's view of the harms they can be caused that the organisation has to take on within its business cases even though this is of a different nature to the organisation centric view of the value of the information.

As we discuss below (see "Scaling and the use of average values"), this also means that the value that needs to be derived under this perspective is set by the maximum harm a person could realistically be caused by any privacy failure. The value figure is not the average harm people could be caused, neither is it the maximum harm people could reasonably be caused but only by the most common privacy failure.

People's attitudes and sensitivities to privacy vary enormously, as do the ways in which people could be harmed if their information is not used as they would wish. This makes quantifying this 'people' dimension of value very difficult. One way to gauge this value is to relate it to the way people might react if they felt their privacy was not being protected. The way in which the organisation treats people's personal information is an influence on the way people feel they are being treated by the organisation. If employees do not feel they are being treated well by their employer, they could fail to show expected levels of initiative, enthusiasm or concern, and this could damage the organisation's success. If customers do not like the way they are being treated by a supplier, they might look for opportunities to take their custom elsewhere. If citizens do not like the way they are treated by a public sector organisation, they could become uncooperative and make the organisation's mission harder to deliver. Where feelings such as these are shared between people, they could poison the organisation's reputation and undermine the trust the organisation relies upon for its success.

As before, each organisation has to assess for itself how its public could be affected by privacy failures. The discussion below of the consequences of privacy failures and the calculation sheet available at Appendix C can help organisations to determine the personal value figures that are right for their operations and processes. At a minimum, each organisation should be able to assess the value of personal information to its employees by examining examples which bear on employees both from the organisational and personal viewpoints. For example, if an organisation's Board member had a sensitive medical condition that was recorded for possible need in an emergency, how much would they consider spending to ensure this information was not used or accessed in an unauthorised manner?

3 – Value to other parties

Personal information can be of value to other parties. These could be parties that have legitimate purposes for using the information, such as those involved in the delivery of a service to an individual, or parties that have wrongful or improper purposes in mind (e.g. criminals, competitors, disaffected employees, gossipmongers, hackers, investigation agencies, detractors). The organisation is custodian of people's personal information and has a duty to provide the correct information in a timely manner to other parties that do have a proper right to use that information, and to protect that information from misuse and abuse by other parties that do not.

The value of personal information from this perspective can be thought of as its 'assurance' value. It is quite similar in some regards to the value determined under the preceding two perspectives insofar as it relates to the magnitude of the damage that could be caused to people by non-malicious

privacy failures, this time by a third party rather than by the organisation itself. However, what is new is the addition of damage assessed from the perspective of personal information getting into the hands of unauthorised other parties and then being misused or abused. Examples include identity theft and financial fraud, harms that clearly would be most unlikely to arise from improper processing performed by the organisation itself but that could arise from the abuse of personal information by other parties. To capture the different threats and, therefore, the different types of harm, the organisation has to assess the value under this perspective separately from the value it assesses under the preceding two perspectives. The chart above shows a number of possible such measures of the harms that can be caused.

As in the previous category, the harm caused to people can sometimes seem to be only loosely related to the value of the personal information in isolation. For example, unauthorised parties might already hold additional information that, when combined with personal information acquired from the organisation, increases that information's value or helps them to identify and cause harm to individuals. It is therefore just as challenging as under the previous perspective to estimate this component of the value of people's personal information.

The chart above also shows the relatively low 'open' market price for stolen personal data. However, the market price of personal data is not related to the harm that could be caused to people. For this reason, it would be a mistake to take the market price of personal information as an indicator of its value.

Separately from any harm that might be caused to the people affected, the organisation itself might be harmed, and the organisation needs to consider that harm too. This could include the reputational damage caused when the data loss is made public or, at a lower level, the embarrassment that could arise when it becomes known that the organisation was not taking adequate care over the personal information it shared with other parties. It could also be competitive harm if, say, the personal information acquired by a competitor enabled them to steal customers or see how the organisation's customers were responding to a recent initiative.

As suggested earlier, one way to gauge the value of personal information is to consider what might happen if people's personal information was not being properly protected. Given the particular type of personal information being valued, consider how people might react if they were to find out that the organisation had made errors in its sharing practices or had allowed their personal information to be stolen, lost, transferred without their permission, or left unprotected and at risk. Would they be annoyed, would they be angry, would they be outraged? Would this be front-page news of a local or national newspaper or would it just make the middle pages of a trade magazine? If a competitor or hostile pressure group were to obtain that personal information, could they cause harm to the individual through the organisation (e.g. change or corrupt that information) or nothing more than embarrassment? Could they cause harm to the organisation itself, for example if the other party were a detractor who wanted to damage the organisation's reputation.

As before, the discussion of consequences and the calculation sheet available as Appendix C can help organisations to determine the value figures that are right for their operations and processes.

4 – Societal value

UK citizens value privacy and privacy is an important aspect of the relationships between people and government, between one organisation and another, and of ensuring competitive marketplaces³. As explained in the main report, the societal value of personal information manifests itself in two ways: as the organisation's desire "to do the right thing" and as the value given to the protection of privacy by regulators.

With regard to the organisation's desire to "do the right thing", this may form a major component of the culture of the organisation and of the reputation the organisation projects to its public⁴. The value of "doing the right thing" derives from the fact that it has a powerful influence on the confidence, trust and loyalty people, both within and external to the organisation, feel. To gauge that value, consider the contribution "doing the right thing" makes to the organisation's success, the effectiveness of its operations and its ability to implement strategic change successfully when needed.

With regard to compliance, data protection agencies (the ICO in the UK) have a duty to ensure that the public's interests are protected by all organisations holding personal information within their jurisdictions. Compliance commonly requires a wide range of controls to ensure not only that data is secure from theft or loss but that it is gathered only under suitable conditions and used only under suitable restrictions. The value of personal information here arises from the possibility that a breach of legislation could lead to censure, reputational damage, fines, restrictions on operating licences, and in the future even jail terms for senior personnel. Whilst the societal culture and legislation in other countries may be different, and in some countries privacy is treated as having great value whereas in others it is treated as not being of much value at all, multinational organisations might find a privacy failure in their overseas operations affects their reputation elsewhere in the world. Hence, while the direct impact (censure, fines) might vary with jurisdiction, the effect on reputation could be much the same regardless.

"... if citizens have an underlying fear that their data may be lost or stolen they will not participate fully in the digital economy. ... Those who profit from the information revolution must respond to the public policy responsibilities that come with it."

Viviane Reding⁵, Member of the European Commission responsible for Information Society and Media

Many sectoral regulators also have a strong interest in seeing the sector uphold high standards of privacy practice and can impose large penalties of their own for privacy failures (introducing the possibility of double jeopardy). For example, financial services organisations can be fined for taking an insufficiently strong approach to the protection of data in general by their regulator. It is also important to bear in mind that it is not necessary for an incident to occur for a breach of regulation to have taken place.

³ Kenneth Laudon, Association for Computing Machinery. Communications of the ACM; Sep 1996; 39, 9, <http://www.eecs.harvard.edu/cs199r/readings/laudon.pdf>

⁴ True Colours, Uncovering the Full Value of Your Organisation, National Council for Voluntary Organisations, March 2008, <http://www.ncvo-vol.org.uk/products-services/publications/true-colours>

⁵ Securing Personal Data and Fighting Data Breaches, Speech at EDPS-ENISA Seminar 'Responding to Data Breaches', 23 October 2009, http://ec.europa.eu/commission_barroso/reding/docs/speeches/2009/brussels-20091023.pdf

The chart above shows the magnitude of some of the fines the Financial Services Authority (FSA) has imposed for recent data security (not strictly privacy) failures and the current fines for criminal DPA offences. In 2009, the FSA consulted on its policy for determining enforcement financial penalties and changes are expected to be implemented by spring 2010⁶. At the time of writing, the increased fines⁷ ⁸ that the ICO will be able to impose on organisations that seriously contravene the Data Protection Principles and where this is likely to cause substantial damage and distress. However, fines notwithstanding, for most organisations, the primary source of societal value is the loss in reputation caused by adverse coverage in the media.

Scaling and the use of average values

When developing input to a business case, scale is important to some of the numbers being developed. For example, the benefits from exploiting personal information as an asset might well scale in direct proportion with the number of customer records being used, and the costs involved in dealing with a privacy failure might well scale with the number of people whose privacy has been affected. The value of personal information does scale in some ways with the number of records being considered but organisations need to be very careful how they perform that scaling.

The value to the individual

When looking at the value of personal information to the individual, value is a reflection of the magnitude of the distress or harm that could be caused to individuals if their privacy is violated. The actual harm or distress that would be caused to any one individual by any one incident would vary widely from individual to individual, by the type of personal information involved and by the nature of the privacy failure. If an organisation is handling a large number of records, faced with this wide variation in individual values it might be tempted to take an average value as an indicator of the per record value of personal information and scale that figure up by the number of personal information records they handle.

However, using an average in this way would not be a safe approach. The value of personal information in this perspective is set from the individual's viewpoint not from the perspective of the organisation. For each individual who could be affected by a privacy failure, it is the potential distress and harm they as an individual could suffer that is important to them, and it is that that sets the value of their personal information. No person would be satisfied being told that the protection they will be given is limited to just an average level of harm they might suffer taken over many people other than themselves. They would insist that the value of their information to them and the level of protection they should expect is set by the greatest possible harm that they fear they as an individual could suffer. Therefore, the correct per record value to take when valuing personal information from the perspective of the individual is the maximum harm an individual could reasonably suffer, not an average harm.

6 FSA Proposes Bigger Fines to Achieve Credible Deterrence, Press Release, FSA, 6 July 2009, <http://www.fsa.gov.uk/pages/Library/Communication/PR/2009/091.shtml>

7 ICO Welcomes New Powers to Fine Organisations for Data Breaches, Press Release, ICO, 9 May 2008, http://www.ico.gov.uk/upload/documents/pressreleases/2008/criminal_justice_and_immigration_act.pdf

8 Information Commissioner's Guidance About The Issue of Monetary Penalties Prepared and Issued Under Section 55C (1) of the Data Protection Act 1998, ICO, 12 January 2010, http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_guidance_monetary_penalties.pdf

The number of records

A second approach an organisation might be tempted to take when dealing with the wide variation in harms people are likely to be caused is to assume that not all people affected by a privacy failure would be harmed by that failure. If a million financial records were stolen by a fraudster, it is unlikely that all one million people would subsequently be the victims of financial fraud. The organisation would then take just a part of the total population potentially affected as the number by which to scale the individual person's value. Hence, an organisation that handles a thousand people's personal information might make the assumption that, say, only ten percent of those people would actually be affected by any particular privacy failure that might occur and that they could scale the information's per person value by a multiplier of one hundred not one thousand.

Again, this would not be a safe approach. The value of personal information is set by the scale of the harm that could be caused and that is set by the possibility that all the people whose privacy is violated could be harmed by that failure. The cost to the organisation of dealing with the failure might well scale with the number of people actually harmed by the failure, but value is not to be confused with cost. The value of the personal information has to scale with the full number of people who might be affected by a privacy failure, not an estimate of how many are thought likely to be affected on average.

Quantification of the value

A calculation sheet is provided in Appendix C to aid the calculation and comparison of personal information's value from each of the four perspectives discussed. Notwithstanding all the cautions that need to be observed when dealing with averages, in practice, a single numerical average value is often sought. Here we consider what that value might be.

The total value of personal information to the organisation may be hundreds, thousands or millions of pounds, but the data brought together in Figure S1 appears to suggest a typical commodity value per record is likely to be in the £10-£100 range. The value to other parties who do not have a legitimate interest in personal information appears to range from a few pence to £100.

From a person-centric viewpoint rather than an organisation-centric one, the value of an individual's own information could be much higher, typically in the £100 to £1,000 range per person. If we consider financial fraud, where there are data published⁹, a recent UK survey¹⁰ suggests that the average financial loss per victim is £463. While any one individual person might be able to recover some or all of this loss, this will not always be the case.

In addition to this loss, an estimate should include the time and expenses of the person affected, and other resultant non-financial harms such as loss of opportunity or health side-effects from their worry and sleepless nights. The available data suggest¹¹ it typically takes between 3 and 48 hours for a victim of identity theft to clear their name and return to normal. If this time is costed at both typical

9 Measuring Identity Theft, Workshop Report, Identity Theft Prevention and Identity Management Standards Panel, American National Standards Institute, October 2009, <http://webstore.ansi.org/identitytheft/>

10 One in Eight Brits Fall Victim to Online ID Fraud, Press Release about YouGov survey, Verisign 16 September 2009, http://www.verisign.co.uk/press/page_20090916.html

11 Identity Fraud and Identity Theft, CIFAS, 2008, http://www.cifas.org.uk/default.asp?edit_id=968-56

non-working time market price¹² and mean weekly earnings¹³, this would indicate, as shown in the worked example in Appendix D, the average cost to the victim (the sum of their financial loss and the time and effort needed to correct the results) amounts to between £476 and £1,054, or say between £450 and £1,050. To this should be added an allowance, say £50, for the other expenses and potential harm effects not otherwise included, giving a total average value in the range £500 to £1,100.

12 Department for Transport, <http://www.dft.gov.uk/pgr/economics/rdg/reportonworkshoptraveltimes1081?page=3>

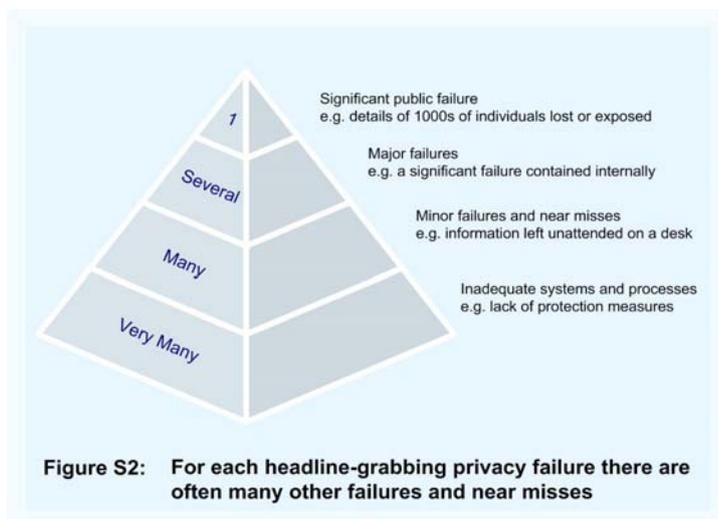
13 2009 Annual Survey of Hours and Earnings, Office for National Statistics, <http://www.statistics.gov.uk/statBase/product.asp?vlnk=15313>

The consequences of privacy failures

Privacy failures damage business. Here we help organisations to understand the forms that damage could take for them. Appendix E contains a calculation sheet to help organisations estimate the costs associated with these.

Approach

Privacy failures are not uncommon. Surveys¹⁴ suggest that most large organisations have at least one significant data loss (also commonly referred to as a "data breach") a year and many have two or more, maybe even a dozen.



Furthermore, it is well understood that reported data losses represent only a fraction of those that occur. For each significant headline-grabbing incident, it is probable there are several other major failures going unreported and many more minor failures and near misses (see Figure S2). And, as already mentioned, data losses account for only one of the many types of privacy failure organisations need to consider. It is only sensible to expect that other types of privacy failure also follow the same or a similar general distribution.

It is only sensible to expect that other types of privacy failure also follow the same or a similar general distribution.

If an organisation has good controls in place, privacy failures are less likely to take place than if not. But privacy failures can and will still happen. And it is not just the large, publicly-visible failures that could hurt the organisation, the costs of the many less serious ones need to be included in the calculations too. The costs to the organisation of suffering privacy failures are very real, and, as will be explained in the next section, the avoidance or reduction of these costs is, for most organisations, one of the main benefits they could realise from protecting privacy better.

Often when people think about privacy failures they think in terms of specific events that could occur: data being lost; customer information being misused; people being unfairly excluded. However, it is not so much the failure event as the failure consequences that cause whatever damage ensues. It is the consequences that need to be considered when building a business case.

To get a measure of the damage consequences can cause, it is important to think in terms of privacy failures in general rather than to imagine the particular consequences of any specific failure. No two privacy failures are ever the same. Even if records have been kept of the various costs associated with a particular failure in the past, these can only be general indicators of the costs that might be incurred in the future, even for a similar type of failure. And, as the amount of damage caused by

¹⁴ See, for example, the Ponemon/PGP 2009 Annual Survey on UK Enterprise Encryption Trends, http://www.pgp.com/insight/research_reports/index.html and the BERR Information Security Breaches Survey 2008, <http://www.security-survey.gov.uk/>

each failure can vary enormously depending on the specific details and context, the range of costs will be wide. Hence, the aim is not to try to estimate the exact costs of each particular privacy failure but rather to estimate broadly the costs that might reasonably be expected due to the wide range of privacy failures that might reasonably be able to occur.

Consequences

Privacy failures have consequences and these consequences affect the business in several ways. Failures can have direct consequences: those incurred as the individual failure plays itself through from incident to closure. They can have indirect consequences: those which follow as people adjust their attitudes and behaviours towards the organisation. And they can have wider consequences, where one organisation's failures could affect other organisations associated with it. Privacy failures could also have deferred consequences. This is where the privacy failure does not lead to a specific incident itself but instead increases the likelihood of other future incidents occurring. An example of this would be excessive retention of personal information. Though not an "incident" itself in the sense of an event that causes immediate harm, it increases the organisation's vulnerability to future mistakes that might happen leading to privacy failures and concomitant consequences.

We consider each of these types of consequence in turn. Here we outline what these consequences could be so each organisation can estimate the costs they might face and determine which are likely to be the most costly or have the most influence within their organisation. In Appendix E we provide a calculation worksheet that can help an organisation to quantify the damage privacy failures could cause.

Direct consequences

These are those that follow directly as each failure plays itself through from initial incident to resolution and closure. Those that should be considered include:

- The diversion, at probably zero notice, of senior management and key support staff time and attention to dealing with privacy incidents. Everything else they were planning to be working on, for however long the failures take to play out, will suffer.
- Triage and initial response to contain the privacy failures. A wide range of personnel (e.g. public relations, legal, personnel, security) can become involved in the initial responses to serious incidents.
- The disruption to the normal operation of affected business processes while the privacy failures are being contained. Whilst the disruption is likely to be largest in the early stages of a failure, some disruption could persist for an extended period of time.
- The effort and cost incurred dealing with each specific incident. In addition to the personnel costs already mentioned this can include:
 - The cost of notifying affected or potentially affected people.
 - The cost of providing those people with additional protection (such as financial monitoring services) or recompense or remedy if the personal information was particularly sensitive. As already mentioned, the consequences on individuals can

be difficult to predict and can vary widely between individuals. Hence, do not take an average value for this harm as that does not provide a meaningful estimate of the organisation's exposure.

- The cost of running internal investigations to identify root causes and responsibilities for failures.
- The cost of providing detailed reports to regulators and the ICO.
- The cost of supporting one or more external investigations (by a regulator, the ICO, other agencies).
- The impact that flows from those external investigations (e.g. legal costs, fines, penalties, restrictions on future operational freedom).
- The effort and cost incurred ensuring failures are not repeated. Corrective measures will need to address root causes rather than just the individual cause of each particular incident, and will probably need to be applied to a range of information systems rather than just one, as several systems could well be vulnerable to similar weaknesses.

"I'm also annoyed that the responsibility for doing something about this seems to have been passed on to me."

Victim of a privacy failure on the Guardian newspaper's jobs website, BBC News¹⁵, 25 October 2009

The above costs are those associated with the privacy failures that occur. However, as discussed previously, not all of these direct costs require a privacy incident to occur before they are incurred. Mandates such as the DPA do not require there to be a data loss for a breach of the legislation to have occurred. The ICO has shown that it is able to issue enforcement notices on organisations, and the FSA has also shown it is willing to impose financial penalties on organisations, where there has been no loss of data but the organisation is judged nonetheless to have inadequate controls in place.

Indirect consequences

These are those that follow as people and the organisation's partners adjust their attitudes and behaviours towards the organisation. Those that should be considered include:

- Reputational damage and loss of trust by the public:
 - Brand damage. The brand is an asset and requires continual maintenance. Brand damage can take a long time and significant cost to reverse.
 - Loss of returns (i.e. loss of business revenues or a reduced take up of a service provided). A public sector system or service that fails to achieve planned levels of adoption represents a loss. In the private sector, customers may take their business elsewhere. Prices charged might need to be reduced to staunch the outflow of customers.

¹⁵ <http://news.bbc.co.uk/1/hi/uk/8324630.stm>

- The company's equity value can be impaired for a period¹⁶. Studies looking into the negative impact on share prices for companies that have suffered a major privacy failure have not been particularly conclusive. It appears that the impact is greatest where customers have lower switching costs, and the effect is usually reversed with time. However, the impact can be significant for a period, and can affect operating costs such as the cost of raising finance.
- Reduced effectiveness of information systems and processes (see the boxed example below). When people do not have confidence in the organisation to which they are providing personal information, they apply defensive tactics such as withholding information or providing false information to counter their increased sense of vulnerability. This costs the organisation time and money and limits the usefulness of the information it processes. If the personal information is used for strategic purposes, this also limits the strength of the decisions made.

Linking individual empowerment with business success

Empowering individuals to take control of their data can produce benefits to the organisation. The other side to this coin is that making it hard for people to do what they want to do can generate consequences.

Some organisations make it difficult for people to opt-out of, or change their communication preferences, and the effects of this can be wider than might initially have been expected. Take for example the situation when a couple are arranging their wedding or civil partnership and they have visited, contacted or registered with a number of companies providing services for the event. Once the event is over, they will normally want to end their relationships with these companies, since they hope they will not be in need of the same services again in the foreseeable future. But if they are unable easily to take their names off the company contact lists not only do they become annoyed or frustrated but the companies incur greater customer support costs and wasted future marketing expense.

There could be further consequences. Complaints might be raised about direct mail or additional telephone calls leading to censure by the press, a regulator or trade organisation. Emailed correspondence might be marked as spam, and if enough people do this, the ability of the organisations to deliver their service and marketing messages will be reduced since their email deliverability would be impaired.

- Increased operating costs. Maintaining customer relationships might become more expensive (see boxed example below). Employees might become demotivated leading to poorer performance, higher churn, increased retraining and management costs. It can be harder to recruit new high-calibre employees.
- Reputational damage and loss of trust by business partners.
 - Loss of existing business. Customers or suppliers might terminate contracts, especially if the organisation loses a relevant certification (e.g. is removed from the PCI list of certified processors) or its operating licence.
 - Loss of opportunity and future business as, both, the organisation's current

¹⁶ Is There a Cost to Privacy Breaches? Alessandro Acquisti and Rahul Telang, Carnegie Mellon University and Allan Friedman, Harvard University, 2006, <http://weis2006.econinfosec.org/docs/40.pdf>

partners and new ones it might hope to replace them with, lose confidence.

- Increased scrutiny from business partners and increased costs of obtaining and maintaining their support or services, or delays to contracts being placed.

The effect of trust on sales channels

The knock-on effects of an event like a privacy failure can impact significantly on operations. Consider an organisation that sells through a number of channels including e-commerce. The consequences of an online privacy failure might undermine trust in the organisation or just the e-commerce channel. In an organisation where its only sales channel is e-commerce, such as a price comparison website, the effect on the organisation would be immediate and terminal.

If, rather than causing customers to go elsewhere it led to customers shopping through the organisation's high-street stores instead of its on-line stores, the sudden shift in demand to the physical channel would have to be catered for despite the higher transaction costs to prevent the loss of revenue and customers.

In the public sector, consider the same scenario for a government agency like the DVLA. In 2008-09, almost half (17 million) of all vehicle licensing transactions were undertaken using the web-based Electronic Vehicle Licensing (EVL) system, and the peak number of total transactions grew to 130,000 per day¹⁷. If a loss of trust caused even a small shift of this traffic back to other channels, the impact on the DVLA would be huge: higher processing costs, reversing the 10-15% drop in unit transaction costs already achieved¹⁸, and an increase in face-to-face transactions at post offices possibly leading to the DVLA having to renegotiate its contract with Post Office Counters Ltd.

The impact on the economy would be large too. The introduction of EVL has been a significant contribution to the Department for Transport's Simplification Plan¹⁹ target to reduce by 25% the administrative burdens that their regulations place on business by 2010. EVL alone is estimated to be saving UK businesses nearly £14m each year²⁰. A shift back to people using the Post Office instead of going on-line would increase costs to organisations and individuals alike.

Wider consequences

One organisation could be affected by the privacy failures of another. Though these can be difficult to predict, each organisation needs to give some thought to these consequences in case they do illuminate an otherwise overlooked risk.

Firstly, trust can be felt for a whole sector rather than just a single organisation. So can distrust. As a result, all of central government could be tarred to some degree by a large privacy failure in a single department; all card processors could become a bit less trusted following a single incident involving millions of card accounts; the growth of a new market could be held back by the public distrust generated by a single careless organisation; distrust or a perceived lack of concern within a sector could lead to an increase in regulation and bureaucracy; a local economy and perhaps the UK economy as a whole could suffer if it is not considered a good place to undertake business.

17 Annual Report and Accounts, 2008-2009, Driver and Vehicle Licensing Authority, page 29, <http://www.dft.gov.uk/dvla/~media/pdf/publications/AR%20R%2008%2009%20web.ashx>

18 Annual Report and Accounts, 2007-2008, Driver and Vehicle Licensing Authority, page 43, http://www.dft.gov.uk/dvla/~media/pdf/publications/Annual_accounts2007_2008.ashx

19 Simplification and Better Regulation, Department for Transport, December 2006, <http://www.dft.gov.uk/about/eibr/simplificationplan/>

20 Annual Report and Accounts, 2008-2009, Driver and Vehicle Licensing Authority, page 30, <http://www.dft.gov.uk/dvla/~media/pdf/publications/AR%20R%2008%2009%20web.ashx>

A strong UK economy benefits organisations

Protecting privacy contributes to the Government's vision of making Britain a fairer, stronger and more prosperous society²¹. If organisations can reap the benefits of proactive privacy protection, they will be better placed to compete in the new economy and when combined with world class public services²² will contribute to making the UK the preferred place to do business²³.

Secondly, an organisation might suffer some of the direct and indirect impacts of a privacy failure even if it was not the cause of the originating incident. If a subcontractor is the source of the privacy incident but it is the primary organisation's public who are affected, then it is the primary organisation's name that will be associated with the incident.

Though difficult to account for within a business case, the fact that 'cross-contamination' can occur in these ways can only increase privacy risks.

Consequences in the business case

The consequences considered when making the business case end up as costs that might arise in the future as the result of privacy failures. Improving privacy protection should reduce the likelihood and impact of privacy failures and hence reduce the aggregate or annualised costs associated with failures. Therefore, the costs associated with these consequences can be treated within the business case as costs expected if not implementing the proposed privacy improvement and, suitably scaled down, as benefits if implementing the proposed privacy improvement.

21 Building Britain's Future, HM Government, 29 June 2009
http://www.cabinetoffice.gov.uk/newsroom/news_releases/2009/090629_bbf.aspx

22 Excellence and Fairness: achieving world class public services
http://www.cabinetoffice.gov.uk/media/cabinetoffice/strategy/assets/publications/world_class_public_services.pdf

23 Digital Britain Report, 16 June 2009
http://www.culture.gov.uk/what_we_do/broadcasting/5631.aspx/

The benefits of protecting privacy

Protecting privacy brings benefits to the organisation. Here we help organisations assess what those benefits could be for them. Appendix F contains a calculation sheet to help organisations to estimate the magnitude of the benefits they might expect to see.

Approach

Protecting privacy benefits the organisation when it helps the organisation be successful or achieve its business objectives. Different organisations will have different objectives but for many, these will include: increase resilience; increase returns; reduce operating costs; reduce risks. Organisations also need to ensure compliance with privacy mandates. We will look at how protecting privacy could provide benefits in each of these areas.

As each organisation works through the possible benefits to determine the magnitude of these for them, they need to have in mind the extent to which privacy will be protected within their organisation. As explained in the main report, organisations have options regarding how ambitious an approach to privacy they take. Being ambitious and protecting privacy “by design” should amplify the size of the benefits achieved, more than compensating for any additional costs incurred.

Benefits

Increase resilience

Organisations should measure trust not just in terms of the level of trust achieved but also in terms of its resilience in the face of unfavourable events. Deep trust may take a long time to develop but once in place it can withstand a wide range of challenges. The impact of any one privacy failure on the level of trust people feel and the effect it has on the organisation’s operations may not be directly measurable. However, the combined result of a number of failures over a period of time could be the eventual and sudden collapse of trust, with all the implications for costs and efficiency that brings. Once lost, that trust is then very difficult to recover. As with deep trust, deep distrust can be extremely resilient to change. A huge effort and cost, and enormous persistence in the face of little apparent return, is needed if trust, once lost, is to be recovered.

Protecting privacy strengthens and deepens the trust people have in the organisation. It helps to sustain the organisation by strengthening its resilience and that helps to ensure continued success in the face of all the many trials and tests the organisation is exposed to from day to day, year to year.

The benefit of increased resilience is hard to quantify but of notable value nonetheless, and it should be an important component within a business case.

Increase returns

How the organisation handles people’s personal information is central to the degree of trust on which the relationships the organisation has with the people it serves are based. Protecting privacy builds trust and strengthens those relationships, making them more long-lasting and productive. It also strengthens the organisation’s reputation and that helps to attract new customers. In the words of

Ann Cavoukian, the Information and Privacy Commissioner of Ontario, Canada²⁴, “The ‘payoff’ to privacy-respecting organisations is ... ultimately, enduring competitive advantage. In a world of increasingly savvy and inter-connected customers, an organisation’s approach to privacy may offer precisely the competitive advantage needed to succeed.”

In the private sector, it is well understood that increased trust and loyalty lead to a higher volume of sales over a longer period of time. Customers are more likely to keep returning for subsequent purchases. In businesses where the cost of switching provider is low, customer satisfaction is key to retaining customer business long enough to generate a good return on the cost of customer acquisition.

Better privacy protection could provide an organisation with the opportunity to differentiate itself from others. Customers prefer to deal with businesses they can trust as that reduces the ‘cost’, as they experience it, of the relationship they have with that business. Being willing to pay a premium for the offerings made by a trusted organisation is how a share of the value generated by that trust is returned to the organisation that generates it.

In the public sector, trust and public engagement is a prerequisite for government systems to work. Greater trust leads to more rapid and complete take up of services across the population being served. For the voluntary and charitable sector, trust is essential to sustain both donations and the labour people contribute altruistically.

Across all sectors, when people trust an organisation, they are more willing to provide accurate and complete personal information. This increases the value of that personal information to the organisation, helping to create opportunities for new services and improving the soundness of the strategic decisions made.

Reduce operating costs

Just as protecting privacy makes the relationships an organisation has with its public more productive, it also makes them easier and less costly to manage. People are more willing to provide accurate and complete personal information, and are less likely to impose tactical restrictions of their own, as they feel less at risk, reducing the organisation’s information assurance costs. They are more likely to have a positive attitude towards the organisation, reducing the costs of maintaining those relationships (e.g., making it easier to manage calls to customer call centres). Having a better reputation reduces the costs of customer acquisition and reduces churn.

Protecting privacy builds trust and strengthens the psychological contract between the organisation and its employees. Strengthening employer-employee relationships makes them more long-lasting, reducing recruitment and training costs. It helps to make those employees more hard working and productive. And it makes it easier to attract new, high quality employees.

Research shows that as people increase their awareness of privacy matters, their sensitivity to how their information is handled and to the respect with which they are treated increases. Privacy awareness is expected to rise as the UK becomes more and more a digital society. This will increase all the above benefits of addressing people’s personal privacy concerns properly.

²⁴ Privacy by Design, Ann Cavoukian, Information & Privacy Commissioner, Ontario, Canada, January 2009, <http://www.ipc.on.ca/images/Resources/privacybydesign.pdf>

Reduce risks

Protecting privacy reduces the security risks to the personal information being held and to the organisation's reputation. It does this in two ways.

Firstly, by being aware of the special value that personal information has for people, organisations typically afford personal information a higher security classification than they might the non-personal information used alongside it. This leads directly to higher standards of security being applied and reduces the risk of security failures taking place with personal information.

Secondly, many of the steps organisations take to protect privacy have the effect of reducing their vulnerability to security threats. An organisation is less likely to collect personal information it does not need, less likely to allow personal information to travel widely within the organisation, less likely to perform unnecessary processing on that information, and less likely to retain that information longer than is necessary. All of these reduce its vulnerability to security threats.

The correlation between protecting privacy and reducing security risk is proven. "Companies with documented procedures to ensure compliance with the DPA are half as likely to experience data protection infringements, unauthorised access or confidentiality breaches by staff as those that do not"²⁵.

In addition to reducing security risks, improved privacy protection could lead to a reduction in other types of risk such as operational, strategic, project and market risk. The range and magnitude of this effect will vary considerably according to the particular circumstances of the organisation. They might include, for example, reduced risks of employee non-compliance, or reduced risk of a new offering not being taken up by customers.

Improve compliance

The DPA applies to every organisation in the UK that processes personal information and no organisation should believe that it has the right to ignore its legal obligations. Compliance is not a commodity to be traded on the basis of whether the costs of non-compliance are greater or less than the returns that might be gained from using personal information in a non-compliant manner.

However, organisations do still face, and need to manage, the risk that they might be found non-compliant with an external mandate. As external mandates usually apply to a broad range of organisations, they are rarely prescriptive and this introduces the risk of unintentional non-compliance. The benefit of a positive approach to privacy protection that aims to exceed minimum requirements is that it reduces this significant risk.

The benefit of ensuring compliance with the DPA extends beyond the simple avoidance of the fines and other penalties associated with non-compliance. Various stakeholders²⁶ impose additional obligations on organisations relating to their compliance with data protection law²⁷. This can include requirements to report on the protection of personal data in annual reports, and to report on the privacy protection measures organisations have in place. A reduced risk of non-compliance could

²⁵ The Information Security Breaches Survey 2008, BERR, <http://www.security-survey.gov.uk/>

²⁶ See Appendix G

²⁷ Data Handling Procedures in Government, Final Report, Cabinet Office, June 2008, http://www.cabinetoffice.gov.uk/reports/data_handling.aspx

lead to more straightforward reporting and avoid putting the benefits of the organisation's membership of community or sectoral bodies at risk.

The investment needed for the protection of privacy

Here we discuss in outline the main steps involved in protecting privacy. This is so each organisation can see the full scope of what privacy protection entails, enabling it then to assess how comprehensive a privacy improvement programme it needs to develop and the potential costs it might incur.

Approach

The overall aim of the organisation should be to develop the capability to realise the benefits previously described reliably and effectively. In the main document we recommended a proactive, comprehensive, enterprise-wide approach to maximise the privacy dividend.

Privacy failures can take any of an innumerable range of forms. As should be clear, preventing privacy failures is not just about preventing the unauthorised disclosure of personal information, and privacy protection is not just about encrypting data on portable devices or storage media. Privacy protection is about making sure the organisation has the ability to identify and understand its privacy risks well, and has the skills and strengths it needs to address and manage those risks in a suitable manner irrespective of the particular forms in which those risks manifest themselves. It is about weaving a respect for people's privacy into the fabric of the organisation, and then developing the approaches and methodologies it feels are right so it keeps privacy well protected.

"Privacy protection is not a cost of doing business, it is part of doing business"

Contributor to the report's discussion document

We will not discuss here specific privacy protection measures, techniques or technologies. Those are covered in great depth and detail in the literature available on the Internet and elsewhere. In addition, no two organisations will need to implement the same set of privacy protection measures. There are good reasons why the measures most appropriate to one organisation will not be those most appropriate to another. As a result, we describe here the mainstays of a privacy protection programme. Each organisation will need to develop its own particular methods and practices and to select and implement whatever specific measures, techniques and technologies are best for it.

The mainstays of a privacy protection programme

These are the main steps each organisation should be considering to help ensure it protects privacy well.

- Develop and articulate the vision of what privacy protection means for the organisation.

This will describe, in the organisation's own words, its reasons for respecting personal information rights, the priority it gives to its privacy obligations, and the role protecting privacy plays in supporting the organisation's overall mission. Care should be taken to ensure this vision does not equate privacy protection with information security protection. Reference to the eight principles and individuals' rights in the DPA can help ensure the vision is sound and addresses privacy protection as a whole.

- Develop a clear statement of how privacy governance will be arranged within the organisation.

This does not mean that privacy should necessarily be under the control of a separate or dedicated function; privacy protection is an aspect that contributes to many aspects of an organisation's success and accountabilities and responsibilities can be distributed in many ways. Privacy governance should align with the governance approach practised for other important matters. Otherwise, employees are likely to become confused about roles and responsibilities, important responsibilities might be left unaddressed, and there can be disagreements about leadership and funding.

- Develop and articulate the organisation's primary objectives and chosen approach.

In practice, organisations do not set out to mishandle personal information. Most privacy failures are the result of accidents or mistakes taking place within an environment in which accidents and mistakes are able to happen. Hence, for most organisations, their primary objective will be to create an environment in which employees are less likely to make privacy mistakes and it is harder for accidents and mistakes to play through into actual privacy failures.

However, whether this is the primary objective or just one of several, different organisations will follow different approaches. Each organisation has to decide, for example:

- What the organisation's primary objectives are. Is it to ensure compliance with external mandates, to reduce the risk of privacy failures, or a combination of these and other objectives.
- Which, if any, privacy protection responsibilities are invested in a discrete function or are function-independent and permeating the whole business architecture. If invested in a discrete function, does this function stand in its own right or is it part of another function such as intellectual asset protection, information assurance, or compliance;
- How much is the preferred privacy approach to be proactive rather than reactive, or part of the public brand rather than a purely internal matter;
- The relative priority given to privacy protection objectives and how possible conflicts between privacy and other business objectives are to be resolved;

The objectives and preferred approach should be chosen by consensus amongst all relevant sections of the organisation (e.g., Compliance, Development, Finance, Human Resources, Information Systems, Legal, Marketing, Operations, Procurement, Public Affairs, Research, Risk).

- Develop and disseminate the organisation's privacy principles.

These principles say how the chosen approach will be followed. A number of bodies have developed privacy guidelines and principles²⁸ which they believe to be widely valid and

²⁸ See, for example, the OECD Privacy Principles, the Online Privacy Alliance privacy guidelines; the Liberty Alliance's Fair Information Practices (these organisations are listed in Appendix G).

beneficial, and the organisation should consider to what extent it wishes to adopt each of these. The chosen principles should be documented and then mandated by the Board.

- Develop a privacy protecting culture.

Whatever the chosen approach and principles, they need to become part of the culture of the organisation so they become a natural part of how all employees from all levels approach their daily tasks and responsibilities. Employees should not think protecting privacy is something ‘other people’ do, something that is the sole responsibility of the Privacy (or Compliance, or Information Security) function.

All function heads will need to be involved personally in strengthening and sustaining the culture. Training and awareness-raising materials will need to be available to all employees and tailored to make them relevant and effective for employees at different levels within the organisation (most especially for executives and directors).

- Develop and maintain an understanding of where within the organisation personal information exists.

One weakness for many organisations is that they do not realise how much of their personal information is held in non-structured forms (spreadsheets, word processing documents, desktop applications, and the like). These often exist outside formal information system controls and desktop files are very easy to transmit and exchange “to get the job done”.

If the organisation’s privacy risks are to be managed, it is essential that the organisation knows how and where personal information enters the organisation, how it is stored, where it spreads to, how it is used and what consent has been given, how it is protected, and whether it is archived or deleted when it reaches end-of-life. This lifecycle understanding should include identifying who has responsibility for the protection of which personal information at each stage in the lifecycle.

- Assess privacy risks and implement privacy protection measures.

Once the approach has been defined and the location and uses of personal information understood, privacy risks can be determined and the measures, techniques or technologies needed to protect the information can be chosen. Consideration of proactive rather than reactive, comprehensive rather than minimalist, and enterprise-wide rather than case-by-case need to be addressed and plans developed with related business cases. These need to cover existing systems and business processes as well as new ones.

- Develop, maintain and monitor risk registers.

If the organisation’s privacy risks are to be managed, it is also essential that the organisation knows where its main structural privacy risks are to be found, their order of magnitude and their likely causes. This follows on from, and cannot be achieved without, knowing where within the organisation personal information exists.

At this level, the organisation should be answering broad questions such as:

- Are the organisation’s privacy risks associated mainly with employee personal

information, with customer personal information, or with personal information provided by clients relating to their customers?

- Are these risks associated primarily with IT systems or with manual processes?
- Is the organisation currently very vulnerable to privacy failures occurring (in which case there might be a lot of essential protective work that needs to be undertaken urgently) or is it currently, overall, doing a good job at protecting against privacy risks (in which case its focus might be more on assessing and, where necessary, strengthening its key risk management processes).
- How does the organisation detect, record and monitor privacy failures. Risk levels are extremely difficult to estimate and the best indicator an organisation will have comes from measuring the rate and severity of the privacy failures by which privacy risks manifest themselves. Without this monitoring, the risk register can rarely be more than a 'best guess' estimate.

The enterprise-wide risk register should be supplemented by divisional and departmental risk registers.

- Develop and maintain a privacy protection plan.

For each area of privacy protection activity, keep a running list of the current action priorities and a track of how each of these is progressing. The main areas of privacy protection activity are likely to include implementing, reviewing or improving:

- Employee privacy awareness and training;
- Privacy risk assessments (possibly incorporating PIAs);
- Privacy policies, standards and baselines;
- Compliance assessments for measuring the compliance of information systems and business processes against those policies, standards and baselines;
- The portfolio of various privacy protecting techniques and technologies that are available for implementation within information systems. These will cover a wide range of solutions, from standard text informing people of the organisation's privacy policies through the latest PETs (privacy-enhancing technologies) to comprehensive audit trails so those committing wrongful or careless acts can be traced and appropriate action taken. Some solutions will be best implemented as generic solutions provided at an infrastructure level to all information systems and business processes whereas others will be best implemented as a catalogue of available standard solutions for each information system to use where deemed appropriate.

- Develop and maintain the means for reporting and recording incidents and near misses.

Each organisation needs to have a means by which employees can identify and report privacy shortcomings, near misses and actual privacy failures that they detect within the organisation, both formally when an incident occurs and proactively when

they spot something they don't think is right. Gathering and learning from information about what is not right within the organisation provides the best opportunity to prevent privacy failures from occurring in the future.

- Develop and maintain privacy protection metrics.

The metrics should help assess achievement of objectives, achievement of identified benefits, coverage of the privacy protection plan, occurrence of privacy defects in systems and business processes, occurrence of all degrees of severity and types of privacy failures, the scale, cost and timescale of privacy failures, assessment of third parties, coverage of proactive protection and measurement of external views of the sector and organisation (e.g. media coverage, customer surveys, brand value).

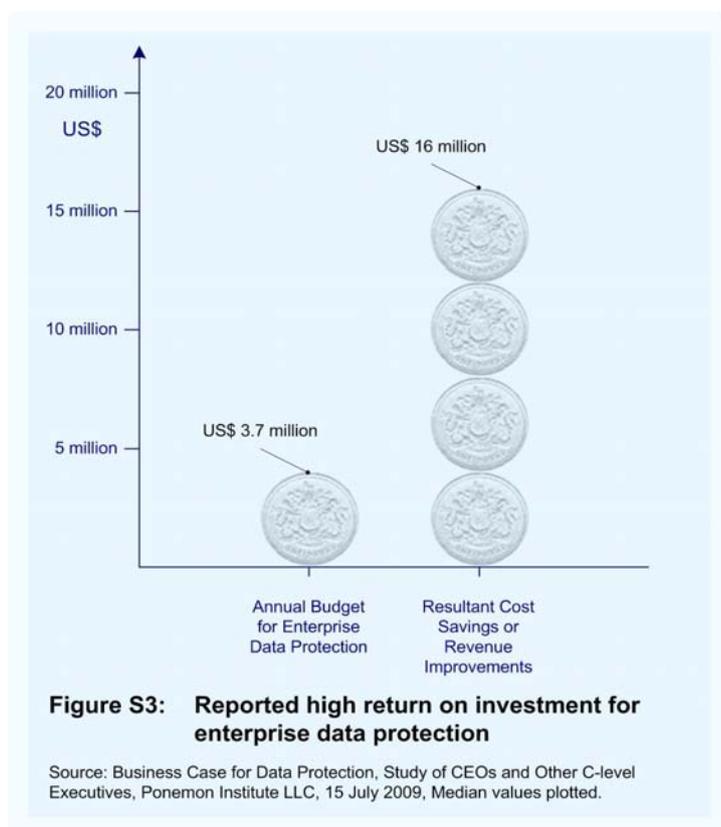
Implementation costs

To make a business case, the rationale for protecting privacy and the benefits that can be accrued need to be qualified by the costs and complexities of achieving protection.

Clearly, the actual costs and complexities that any one organisation faces will be hugely dependent on the drive, size, nature and circumstances of the organisation, and on the amount and urgency of

the work that needs to be undertaken. No generic cost model will be right for more than a small number of organisations. Each organisation will need to develop its own privacy improvement strategy, assisted by the discussion above, and to estimate as best it can what costs and complexities such a strategy might entail.

However, research findings indicate that the return possible on investment in privacy measures could be high. One finding indicated that privacy training is relatively modest in cost, at less than £1 per employee for one very large employer, and highly effective, more so than some investments in technology²⁹. Another indicated that the return on investment for enterprise data protection, where that has been assessed, can be as high as 4 to 1 (see Figure S3)³⁰.



29 Video: How Barclays Improved Security Without Breaking the Bank, Computer Weekly, 5 August 2009, <http://www.computerweekly.com/Articles/2009/08/05/237182/video-how-barclays-improved-security-without-breaking-the.htm>

30 Business Case for Data Protection, Study of CEOs and Other C-level Executives, Ponemon Institute LLC, 15 July 2009, <http://www.ouncelabs.com/PonemonStudy2009>

One of the messages that has featured strongly in the research conducted for this report is that providing privacy protection is closely intertwined with managing personal information well. If personal information is being managed well, then it appears highly likely that the organisation will already be applying many of the measures needed for the protection of privacy.

85% of private organisations believe that the DPA improves information management.
[92% for public organisations]

Annual Track 2008 – Organisations Report³¹, ICO

For example, the organisation is likely already to have an information governance structure in place, to be limiting the collection of personal information to that properly needed, ensuring its accuracy, using it fairly, limiting its dispersal throughout the organisation, protecting it from a wide range of threats, including privacy threats, and, in realising that personal information can be a liability as well as an asset, not retaining it any longer than necessary.

"Removing all privacy protection measures would not make a significant difference to our operating costs, until we had an incident"

Contributor to the report's discussion document

In such a situation, the additional measures needed to ensure the complete protection of privacy are likely to be relatively small in number and the additional costs associated with these measures a relatively small addition. Those organisations which are new to privacy protection and do not have a well developed information management approach will find the costs of implementing privacy protection more significant and more visible.

In the same vein, it would appear to make sense that the complexities of protecting well managed personal information should be less than the complexities of protecting poorly managed personal information. For example, the complexity of keeping an audit trail of accesses to personal information and accounting for any uses made of the information will be less for well managed information than for unmanaged information. Hence, not only is the scale of work required for the protection of privacy hugely dependent on the degree to which personal information is already well managed, but the costs and complexities of additional privacy measures is dependent on it too.

Another factor to be considered when assessing cost is that many of the cost items will take the form of manpower costs rather than procurement costs. Many of the general costs relating to a privacy improvement programme, those which are not specific to individual information systems or processes, are the manpower costs of implementing change within the organisation. Organisations would normally account for these costs differently from how they would account for procurement costs, the latter often being expensed costs, funds leaving the organisation, rather than operating costs such as salaries already committed.

³¹ Report on the Findings of the Information Commissioner's Office Annual Track 2008 - Organisations, ICO, December 2008, http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/ico_annual_tracking_orgs_final_report2008.pdf

Part 2: Creating the full business case

In this part of the supporting document, we explain how organisations might wish to use the materials presented to develop their own specific business cases tailored to their particular needs and circumstances.

Approach

This document provides guidance on creating business cases that address privacy protection for two situations: implementing a new information system or business process, and changing an existing system or business process (either to implement proactive privacy protection or for some other business change). In both cases it might be that some additional spending on privacy protection, over and above meeting minimum compliance requirements, has to be justified.

The guidance is not an explanation of how to write particular business cases, but is instead a description of how the privacy aspects should be incorporated, and where additional information can be found in the main document and elsewhere in this supporting document.

Business cases should not be written until some pre-screening of proposals for programmes and projects has been performed. This screening should include consideration of privacy protection for all plans that impact on systems and business process which hold personal information.

The guidance has been grouped into sections included in most business cases. These may not be identical to an organisation's own requirements, but cover many situations. The sections are:

- Executive summary
- Background and reasons
- Objectives and options
- Assessment of benefits
- Assessment of costs
- Critical success factors
- Investment appraisal
- Implementation and operation

Each of these sections is now discussed in turn.

Generic structure

Executive summary

Executive Summary should be a standalone summary of the key benefits of the proposal, recommending a definite change. The recommendation should be drawn from the comparison of options and investment appraisal (below). Unless the proposal is specifically the implementation of

proactive privacy protection, the executive summary would not have any additional requirements to any other business case. For privacy protection business cases, sufficient information on the business benefits from introducing proactive privacy protection should be identified.

Resources:

- The content in the main business case document

Checklist:

- Define the major benefits
- Use terminology that is understood in the organisation (e.g. "data protection" instead of "privacy protection") but do not package privacy protection only as a security issue
- Consider which problems and opportunities are of most concern to the business case's audience (e.g. customer service, risk reduction, revenue creation)
- Avoid over reliance on the Data Protection Act (DPA) as a business driver or primary benefit – other benefits will be of more interest

Background and reasons

Consideration of the historical background leading to the current situation should define the position that has led to the business problems or opportunities that the business case addresses. This section should discuss fit with organisational strategy and other programmes.

The context for the business case will be different for every organisation. It not only depends on the business sector, culture and objectives, but the also the types of personal information used in information systems and business processes, and who the stakeholders are. An organisation may already have mature processes for privacy protection, or an organisation may be barely DPA compliant, or an organisation may want to improve privacy protection in third parties such as suppliers or in a newly acquired business. The reason may be to meet some objective, other than better privacy protection, but some of the benefits or risks relate to privacy.

The internal and external mandates for protecting personal information should be identified. See Appendix F identifying numerous bodies that impose privacy protection requirements. Consideration should also be made to the fit with other programmes, including those being contemplated and those already being implemented.

Draw on the concepts in Part 1 of this supporting document, especially the sections on the value of information and benefits. Assimilate and modify the text to make it appropriate to the organisation's own strategy and situation.

Resources:

- The content in the main business case document
- The content in Part 1 of this supporting document, especially "The value of personal information"
- Appendix F

Checklist:

- How does privacy protection relate to solving or pre-empting business problems or exploiting business opportunities?
- How does privacy protection relate to the organisation's strategic objectives?
- Is this business case justifying investment in a privacy protection programme separately, or as an addition to some other proposal's requirements?

Objectives and options

The proposal to address the problems or opportunities should be described and the required measurable objectives stated. The proposal should explain how the problems/opportunities discussed previously will be addressed and outline the privacy or other, preferably measurable, objectives. Objectives (or outcomes) could be purely privacy protection related, for example:

- implement proactive privacy protection across all processes to reduce the risk of a major privacy failure from High to Low by [date]
- increase the coverage of personal information leak detection from 80% to 95% of communication channels by [date]
- reduce minor privacy failures by 40% by [date] and major privacy failures by 60% by [date]
- pass an independent audit on DPA compliance by [date]

Even for privacy-specific proposals, the objectives might be framed in more common business terms:

- increase service take-up by 10% in the [year] financial year
- decrease customer churn by 5% by [date]
- improve customer satisfaction measurably
- decrease average enquiry-to-sale time period by 2 weeks by [date]

where these are the achievable benefits of implementing proactive privacy protection measures.

The consideration and selection of viable options will depend upon the scope and objectives. All options should have the potential of meeting the objectives, but their costs, benefits and risk profiles will be different.

A description of viable options for the particular business case might cover alternatives such as:

- building in proactive privacy protection, or not
- retrofitting enhanced privacy protection to an existing process, or only dealing with privacy failures when they occur
- implementing enterprise-wide proactive privacy protection, or system-by-system measures

The alternatives will depend on the organisation's current privacy protection practices and the mandates already identified. Some alternatives that could be considered are:

- do nothing

- build in the bare minimum to meet compliance requirements
- build in comprehensive privacy protection beyond the minimum.

Then, variations on the latter two are:

- do it proactively or reactively
- address each information system and business process in isolation vs. take an enterprise-wide approach and address the many privacy needs consistently across all systems.

Usually the "do nothing" option can be excluded if any of the other options have identifiable benefits. A "do minimum" may be required. For a business case to implement proactive privacy protection, the options to consider, when no other factors affect these, should include:

1. reactive action on a system-by-system basis as failures occur
2. proactive enterprise-wide action
 - a) bare minimum to meet compliance requirements
 - b) comprehensive privacy protection beyond the minimum

These should lead to the identification and assessment of alternative implementation options (techniques and technologies) to deliver the objectives that will generate additional options that need evaluation. Some alternatives may be ruled out and it may be appropriate to address the reasons so the reader can understand why the selected viable options have been selected. Try to avoid indistinguishable options and ensure that sufficient detail is presented on how the alternatives will meet the objectives.

The method of comparing the benefits, costs and risks of different options will be organisation specific and the author should understand their own organisation's requirements in this area before attempting to identify and evaluate benefits.

Resources:

- The content in the main business case document
- The sections in Part 1 of this supporting document discussing how to value personal information, the consequences of privacy failures, and the investment involved in protecting privacy.

Checklist:

- Are all the options viable?
- Can all the options meet the objectives?
- Have the required privacy goals been identified for each option?

Assessment of benefits

Benefits should be identified and linked to the appropriate objectives so they can be reviewed and the options ranked (developed as a process that each organisation will apply to its business

architecture and business processes, as each organisation will get a different answer according to their specific nature and circumstances).

Review the section "Benefits of protecting privacy" in Part 1 of this supporting document with appropriate stakeholders throughout the organisation and identify which benefits are applicable in the organisation and for the particular proposal. Avoid assuming that privacy protection benefits are limited to security and compliance areas – the extra benefits will mostly be seen by other stakeholders such as marketing, public affairs, finance, operations and sales. Whilst there could be many benefits, the practicality of achieving those may make a significant difference between the alternatives identified.

Unless the organisation has standardised methods for converting non financial benefits into monetary values, it is best not to try to change less tangible benefits into fully tangible ones. In practice many tangible benefits can only be predicted with uncertainty, and some cannot be predicted at all. Many of the benefits identified in the primary document are intangible, although there are tangible financial ones too (see Investment Appraisal below).

Try to avoid including mandatory benefits like "DPA compliance" if this is (and should be) common to all alternatives.

If one benefit is a reduction in risk, this may be difficult to measure and thus quantify. For a benefit like this, check how other types of risk are handled in business cases within the organisation. Where all the benefits are intangible, other valuation techniques may be required. A number of methodologies are available^{32 33 34 35}.

Resources:

- "The benefits of protecting privacy" in Part 1 of this supporting document
- Value of personal information calculation Sheet" in Appendix C

Checklist:

- Have all the benefits relating to privacy protection been identified?
- Are the expected timeframes for the benefits defined

Assessment of costs

For privacy protection, the proposal will need to identify the measures, techniques and technologies that will be implemented to gain the benefits and achieve the objectives.

Resources:

- "The investment in protecting privacy" in Part 1 of this supporting document

32 Life Cycle Costing, Office of Government Commerce,
http://www.ogc.gov.uk/implementing_plans_introduction_life_cycle_costing_asp

33 Measuring the Expected Benefits of E-Government, Office of Government Commerce,
http://www.ogc.gov.uk/documents/HM_Treasury_-_Measuring_the_expected_benefits_of_e-government.pdf

34 Appraisal and Evaluation in Central Government, The Green Book, HM Treasury,
http://www.hm-treasury.gov.uk/d/green_book_complete.pdf

35 A Guide to Social Return on Investment, Cabinet Office,
http://www.neweconomics.org/sites/neweconomics.org/files/A_guide_to_Social_Return_on_Investment_1.pdf

Checklist:

- Are the expected timeframes for the costs defined
- Have the costs been distinguished between fixed, variable, semi-variable and step costs?

Critical success factors

Personal information is often referenced by many systems and business processes. An important aspect of a business case will be to determine all the interactions and dependencies with other programmes and projects. The assumptions that are being made for the successful implementation of the proposal need to be documented and assessed. Determine what the consequences might be if these are not realised.

The identification of the proposal's risks and how these impact on the benefits and costs will not be unlike other business cases, but a number of the benefits will be relatively intangible. The constraints on the proposal need to be identified and plans to minimise the risks outlined. Specify here examples of privacy protection risks external to the proposal and project risk events.

Resources:

- "The costs of protecting privacy" in Part 1 of this supporting document

Checklist:

- Have the privacy risks associated with implementing the proposal been identified?
- Have the differences in privacy risks between the options been identified?
- Have the privacy risks of not progressing been identified?

Investment appraisal

The financial appraisal needs to consider the proposal's costs (above) and the financial benefits over appropriate time periods based on either an assessment of the total costs, or the incremental comparison between the options (above), together with a recommendation to proceed with a particular option in the form of a proposal.

The organisation will often have a standard way of comparing options such as using the net present value (at a particular discount rate), return on investment or payback period. Where most of the benefits are not fully tangible, the financial costs may outweigh the financial benefits, but that does not mean the proposal should not proceed—the analysis will help identify the lowest cost option to achieve the other benefits. This means it is very important that sensitivity analysis is undertaken in the financial appraisal.

In privacy protection, where building and maintaining trust can take a long time, it is important not to underestimate the timescales for benefits to be realised, and these benefits should be maintained over much longer periods than the implementation period for the proposal.

Any business case that affects systems and business processes that hold personal information should include identification of changes in risks to the personal information. The author of a business case must understand whether the aim of the case is to justify implementing privacy protection, or

whether it is ensuring that privacy is addressed in the assessment of alternatives along with other factors.

Resources:

- Part 1 of this supporting document

Checklist:

- Ensure that any benefits converted to monetary values have not been double-counted

Implementation and operation

Some aspects of privacy protection such as getting privacy into the organisation culture may take 2-3 years, so depending on the nature of the proposal, it is important not to assume too short timescales. The benefits identified should be clearly benchmarked and targets and timescales set for when they are expected to be realised.

All the resources required for the recommended programme should be listed against the main phases with a high-level targets defined, based on the objectives (above), for the privacy protection programme.

The benefits identified (see above) need to be identified and consideration given to how they will be measured. The business plan should identify the current baselines, targets for each benefit and the timescales to realise the benefits expected.

Methods to determine the continuing viability and believability must be identified.

Resources:

- "The value personal information" and "The costs of protecting privacy" in Part 1 of this supporting document

Checklist:

- Have all aspects of implementing a privacy protection plan been addressed?

Business engagement

A discussion with stakeholders and affected parties is normally useful to identify any further concerns or project risks and to confirm whether assumptions are reasonable. Once the case is finalised, its needs to be presented to the board, group or team responsible for investment decisions.

Part 3: Appendices

In this part, we provide the supporting materials referenced by the business case and within Parts 1 and 2 of this supporting document.

Appendix A - Glossary

The language used in these two documents is UK centric. We have used generic, non sector and non entity-specific terminology to address a broad audience. Here we provide an explanation of how some of these terms have been used. The explanations are not meant to be robust dictionary definitions but are specific to this document.

Employees

The term employees includes all types of human resource in an **organisation** e.g. contractors, directors, management, staff, students, temporary employees, trustees and volunteers.

Organisation

An organisation processing **personal information**. In the private sector any type of organisation including associations, charities, education establishments, partnerships, private and public limited companies, societies, sole traders, trusts and unions. In the public sector, a central government body, local government body or public corporations.

Other parties

Third parties with which the organisation legitimately shares personal information, and **organisations** and individuals with wrongful or improper purposes for personal information.

Personal information

Personal information includes any information that relates to a particular person, whether shared or unique. It is not limited to personally identifiable information (PII). [See also the definition³⁶](#) of personal data for the purposes of the DPA by the Information Commissioner's Office.

Privacy failure

The combination of an event (or action) and a system or process weakness leads to contravention of a privacy protection mandate. This includes all forms of breach of the DPA but also includes breaches of other external and internal mandates.

Public

The individuals about whom the organisation holds personal information. All organisations hold **personal information** about **employees**. For a private sector organisation there may also be **personal information** about customers, donors, members, owners, participants, recipients, shareholders, students, supporters, etc; in the public sector, information about citizens. In both sectors, there may also be information about **employees** in third parties.

Third parties

External **organisations** including suppliers, advisors, outsourcing companies, government bodies including regulators, agencies and local authorities, and partner organisations.

³⁶ Determining What is Personal Data, ICO, http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/personal_data_flowchart_v1_with_preface001.pdf

Appendix B – References for Figure S1

Figure S1 appears on page 5.

1. Business Case for Data Protection, Study of CEOs and Other C-level Executives, Ponemon Institute LLC, 15 July 2009
<http://www.ouncelabs.com/PonemonStudy2009>
Exchange rate of \$0.60/£ used to plot data
2. Press Releases, Financial Services Authority 2007-2010,
<http://www.fsa.gov.uk/Pages/Library/Communication/PR/>
Highest fine £1,610,000, final notice http://www.fsa.gov.uk/pubs/final/hsbc_inuk0907.pdf
3. Maximum fine in magistrates' court for consistent breaches of the Data Protection Act and for notification offences,
http://www.ico.gov.uk/what_we_cover/data_protection/our_legal_powers/criminal_offences.aspx
Note: New powers, designed to deter personal data security breaches, are expected to come into force on 6 April 2010 when the ICO will be able to order organisations to pay up to £500,000 as a penalty for serious breaches of the Data Protection Act,
http://www.ico.gov.uk/upload/documents/pressreleases/2010/penalties_guidance_120110.pdf
4. 2009 Annual Survey: UK Cost of a Data Breach, PGP and the Ponemon Institute, January 2010,
<http://www.encryptionreports.com/costofdatabreach.html>
Breaches by 33 organisations of between 5,200 and 60,000 records
5. HMRC Offers £20k Reward for ID Goldmine CDs, The Register, 5 December 2007,
http://www.theregister.co.uk/2007/12/05/hmrc_offers_cash_for_discs/
£20,000 for 25 million records
6. Security Threats Report, Sophos, 2009,
<http://www.sophos.com/pressoffice/news/articles/2009/07/threat-report.html>
7. Notification, Information Commissioner's Office,
http://www.ico.gov.uk/what_we_cover/data_protection/notification.aspx
Notification fee for new registrations and renewals of £35 per annum or £500 per annum for some large organisations
8. Benchmarking the ICT Service Across The UK, SOCITM, 2008
Referenced in "It's Ours - Why We, Not Government, Must Own Our Data", Liam Maxwell, Centre for Policy Studies, June 2009, ISBN 978-1-906996-00-0,
http://www.cps.org.uk/cps_catalog/it%27s%20ours.pdf
9. Identity Fraud and Identity Theft, CIFAS, 2007
http://www.cifas.org.uk/default.asp?edit_id=968-56
£8,000 cost to victim as upper limit where a total hijack has occurred
10. One in Eight Brits Fall Victim to Online ID Fraud, Press Release about YouGov survey, Verisign 16 September 2009
http://www.verisign.co.uk/press/page_20090916.html
11. The Application Form, Fee and Supporting Documents for a First Adult Passport, DirectGov,
http://www.direct.gov.uk/en/TravelAndTransport/Passports/Applyingforyourfirstadultpassport/DG_174100
12. Credit Industry Fraud Avoidance System (CIFAS) Protective Registration Service for Individuals,
http://www.cifas.org.uk/default.asp?edit_id=874-85
£12 plus VAT (£13.80) per annum
13. How to Access Your Information, Information Commissioner's Office, v1.0, 31 July 2007,
http://www.ico.gov.uk/upload/documents/library/data_protection/introductory/subject_access_rights.pdf
Up to £10, £2 if it is a request to a credit reference agency only for information about financial standing
14. What Price Privacy? The Unlawful Trade in Confidential Personal Information, Information Commissioner's Office, May 2006,

http://www.ico.gov.uk/about_us/news_and_views/current_topics/what_price_privacy_now.aspx
Prices charged to data customers

15. Ministers Plan to Sell Your ID Card Details to Raise Cash, The Independent, 26 June 2005, <http://www.independent.co.uk/news/uk/politics/ministers-plan-to-sell-your-id-card-details-to-raise-cash-496602.html>
16. Discs 'worth £1.5bn' to criminals, BBC News, 28 November 2007, http://news.bbc.co.uk/1/hi/uk_politics/7117291.stm
17. DVLA Sells Your Details to Criminals, Mail on Sunday, 12 February 2007, <http://www.dailymail.co.uk/news/article-369838/DVLA-sells-details-criminals.html>
18. Glut of Stolen Banking Data Trims Profits for Thieves, Washington Post Blog, 15 April 2009, http://voices.washingtonpost.com/securityfix/2009/04/glut_of_stolen_banking_data_tr.html
19. New Estimate of Cost of Identity Fraud to the UK Economy, Identity Fraud Steering Committee, 2007, http://www.identitytheft.org.uk/cms/assets/cost_of_identity_fraud_to_the_uk_economy_2006-07.pdf
20. January to June 2009 fraud figures announced by Financial Fraud Action UK, Press Release, 7 October 2009, http://www.ukpayments.org.uk/media_centre/press_releases/-/page/732/
£232.8m card fraud losses, £39.0m online fraud losses, converted to annual values and 48m UK adults to determine “per adult citizen” values

Appendix C – Value of personal information calculation sheet

An organisation wanting to quantify the privacy value of the personal information it processes can use the following sheets to develop their assessment of the value of that personal information from the four perspectives³⁷. These perspectives are:

- Value as an asset to the organisation
- Value to the individual
- Value to other parties
- Societal value.

Before completing this calculation sheet, the reader is advised to review the discussion of the value of personal information presented in Part 1 of this supporting document.

Where costs, effects or returns might span multiple years, discount these to determine their present worth using a discount rate appropriate to the organisation's financial assessment methods.

For each valuation step, perform sensitivity analysis to determine the effects of any assumptions in the valuation approaches being used. In particular, consider the effect on value as personal information ages, or as the costs used within a particular calculation method change. For each calculation, we have suggested that some assessment of 'confidence' is undertaken and documented; this covers both aspects (quality of data and sensitivity to assumptions).

Based on the scope of the business case being created (e.g., whether an enterprise-wide business case or a case for a single existing business process), identify what personal information is to be included within the business case and the purposes and processing that information is subject to.

³⁷ See 'Privacy value' in the main business case document

Summary

Section	Description
Programme	
Project	
Description	
Valuation performed by	
Date and version	

Once the values from each perspective have been determined, bring forward the values here.

Perspective	Value (£)
Value as an asset to the organisation	
Value to the individual	
Value to other parties	
Societal value	
Maximum of above	

Value as an asset to the organisation

Examine the following methods of valuation and determine which are suitable to the organisation and its personal information. Not all of them will be suitable. Then identify the availability of costing information, and its quality, to understand the level of confidence that can be given to the derived calculations. Where possible, segment the personal information into types, and also within each type segments of value, so that realistic cumulative values and statistical properties can be calculated rather than using simple averages. Each type of information (e.g. employee, marketing contacts, customers) may need to be assessed separately.

Where the organisation does not have its own methodologies for determining the business value of information, there are a number of possible approaches that the organisation might wish to consider³⁸:

Calculation method	Value (£)			Confidence
	Minimum	Average	Maximum	
<p>Cost of acquiring or re-acquiring information of a sufficient quality</p> <p>Would the organisation be able to acquire the information it needs from elsewhere, would it need to go back to the people who own the information to ask for the information it needs, or would it not be able to re-acquire it (e.g. not know who had placed service requests)? Where this is not a market commodity (see below), the cost to obtain all the same personal information, or the amount the organisation would be willing to pay to acquire it.</p>				
<p>Amount of business or mission which relies on the information</p> <p>For example, the present value of expected future returns (e.g. revenue) that would be lost if the information were not available or were not of sufficient quality to be of use. Consider also how strategic decisions would be impacted and the opportunity value that would be put at risk.</p>				
<p>Cost to the organisation if information-based processes are impaired and the organisation has to fall back on more costly contingency or alternative processes</p> <p>Examine of the impact on the organisation if information processes have to be performed in other ways. For example, additional manpower costs, additional third party support costs, the costs of delayed delivery.</p>				
<p>Value of resources being used to store, process, maintain and protect it</p> <p>A guide can be the amount being spent on the lifecycle processing of the information; this is unlikely to be more than the personal information's worth.</p>				
<p>Open market value</p> <p>This may be appropriate if the personal information is available at some standard market price e.g. mailing list data.</p>				

38 Value of Information Subgroup, EURIM, <http://www.eurim.org.uk/activities/ig/voi/voi.php>

Example: Personal information value as an asset to a charity

A UK charity is assessing privacy protection of an existing "customer" relationship management system (CRM) which is being used for interactions with 35,000 donors contributing £2.1m per annum. Legacies, corporate donations, grants from charitable trusts and statutory authorities are managed using different systems. The charity wants to determine the value of personal information in the CRM as an asset.

Cost of acquiring or re-acquiring information of a sufficient quality

The people to contact would not necessarily be known if the information were corrupted or completely deleted. The CRM holds scans of original paper documents and the charity does not pass on its donor's details to other organisations. In the situation where the donor's name and address details are still known but other aspects, e.g. direct debit details are damaged or destroyed, the time and expenses cost to re-contact all of these to check and update the data is determined as £450,000.

Amount of business or mission which relies on the information

One-off donations account for 40% of the income from these donors, and it is expected that in the loss if the CRM or complete loss of its data, with no other external consequences, these one-off donations would be relatively unaffected – the donors just tend to post a cheque or make a donation online. The loss of historical information might have a future effect but this has high uncertainty. Therefore, the calculation is undertaken on the 60% of the income relating to regular direct debits. Whilst these are set up through the banking system, the attrition rate is expected to rise for two reasons. The charity may be unable to renew expiring authorisations and it has no way to contact donors who have stopped their regular payments. The net present value of this loss, allowing for normal attrition rates, is £300,000.

Cost to the organisation if information-based processes are impaired and the organisation has to fall back on more costly contingency or alternative processes

The CRM is a recently new system and the business case for that investment indicated a net present value saving of £600,000.

Value of resources being used to store, process, maintain and protect it

The annualised cost of the CRM, including licensing, support, maintenance and associated staff and management costs is £135,000.

Open market value

The personal information is not available on the open market. Some other charities and third party brokers do have lists that can be purchased, but this does not relate to replacing the information of the same quality. Brokers have lists of individual donors which cost between 5 and 40p per record when purchased in bulk, but these individuals are not necessarily the ones with whom the charity has built up long-term relationships and are therefore most valuable. This method is therefore not considered appropriate.

Conclusion

The value based on an asset to the organisation, is the highest of the above – the cost of re-acquiring it i.e. around £450,000.

Value to the individual

The value of personal information to an individual is set by the level of distress or harm a person could reasonably be caused by a privacy failure arising from the organisation using their personal information within its information systems and processes. As discussed, this is the maximum level of harm that could reasonably be caused by a serious privacy failure, not the average level or the level a common failure might cause. It will be necessary to assess the value from the point of view of the individual based on segmentation into different categories of people and/or damage in the event of failures. Averages should be treated with caution.

For example, it might take an individual a considerable amount of time to provide their personal information (e.g. completing an application for a foreign travel visa) in which case they could be seriously annoyed if they had to repeat the process owing to the organisation's loss of their information.

The damage caused by privacy failures relevant to this perspective can be thought of as the loss of some form of life asset (e.g. time, freedom, wealth, wellbeing) and might include:

- Loss of free time (e.g., people having to put in the time and effort to correct wrong information)
- Loss of freedom (e.g. people being incorrectly detained or constrained)
- Financial loss (e.g., people being denied credit or given adverse terms due to unfair processing)
- Loss of entitlement (e.g. to a benefit, to a service, to goods)
- Physical damage to property or their person (e.g. if given incorrect treatment due to a mix up of records)
- Reputational damage (e.g., as a result of incorrect profiling)
- Emotional stress (e.g. anxiety or the fear of further consequences)
- Embarrassment (if sensitive information becomes known to members of the person's family)
- Intrusion into their private lives (e.g. if incorrectly linked with a crime or extremist group)

Note: the examples here all relate to the effects the organisation may cause to individuals. For harm caused by wrongdoers, see 'other parties' in the following section.

In many cases the direct effects people actually suffer might not be known. However, it is the potential harm that determines the information's value, not the actual harm in the few cases where that might be known.

Calculation method	Value per Individual (£)			
	Minimum	Average	Maximum	Confidence
<p>Cost to the individual of providing their personal information</p> <p>Based on an estimate of the time required to comprehend, gather and submit the information using working or non-working³⁹ values. Business process assessment methods, usability studies or the approach described in the UK Standard Cost Model Manual⁴⁰ can be extended to estimate the time taken for individuals to complete forms or provide information in other ways.</p>				
<p>Damage caused to the individual by a privacy failure</p> <p>All the potential mental, physical and financial harms including the costs of returning to normal over the duration of the impact, calculated as a present value. NB Not effects of a privacy failure involving other parties (see below).</p>				
<p>Value to the individual of providing their information</p> <p>Where it can be determined, the value or benefit the individual might expect to receive in return for providing their personal information or the compensation they might demand if denied that return; it might be possible to calculate this from their view of the value of benefits received in return⁴¹.</p>				
Maximum of above				
Number of individuals				
Total value for all individuals				

39 See, for example, Department for Transport, <http://www.dft.gov.uk/pgr/economics/rdg/reportonworkshoptraveltimeus1081?page=3>

40 Measuring Administrative Costs: UK Standard Cost Model Manual, Better Regulation Executive, Cabinet Office, 29 September 2005, <http://www.berr.gov.uk/files/file44503.pdf>

41 Annex 2, Green Book, HM Treasury, TSO, London and Measuring the Expected Benefits of E-Government, HM Treasury, Version 1.4, 29 August 2003, http://www.hm-treasury.gov.uk/data_greenbook_index.htm

Example: Personal information value to a house seller

A small regional residential estate agent has three branches; two in city locations and one in a nearby village. It holds personal information about its customers which it wants to value. From this perspective, the value to an individual is assessed as the value to a private home owner who has commissioned the estate agent to sell their house.

Cost to the individual of providing their personal information

The estate agent monitored how much time was being spent with each customer from initial enquiry to placing their home on the market and used an estimate of £10-25 per hour to value this time. The personal information exists for current customers but also many previous customers and therefore the number of individuals concerned is quite large. This gave minimum, average and maximum values of £120,000, £240,000 and £300,000 respectively.

Damage caused to the individual by a privacy failure

The estate agent has assessed a number of privacy failure scenarios that do not include the involvement of unauthorised other parties (see next section), The greatest harm reasonably possible appears to be a delay in the sale of customers' homes (i.e. the delay of income) and assumes that the delay does not then lead to the house sales falling through. Based on typical sales values and delays of between one day and one month with an average of 7 days, the minimum, average and maximum values of harm (for all current customers) expected were calculated as £0, £250,000 and £650,000 respectively

Value to the individual of providing their information

The estate agent's customers pay a percentage of the sales price, or a fixed amount for the services performed. This ranges from £3,000 to £15,000 with a mean of £6,500. The market is very competitive with many other estate agents in the same area and pressure on margins from online property services, and therefore it is believed the value to the individual reflects these market costs very closely. The value to the customer is expected to be zero after their house is sold, or they withdraw it from the market. Based on a typical 3-month cycle from signing a client to completion, and allowing for properties which are withdrawn from sale, the estate agents has calculated the minimum, average and maximum values (to all their current customers at any one time) as £150,000, £325,000 and £750,000 respectively.

Conclusion

The value based on the value to the individual, is the highest of the above – damage caused to the individual i.e. around £750,000. The value of personal information to employees and potential house purchases was not determined in this example.

Value to other parties

Determine here the magnitude of the harm that can be caused to both individuals and the organisation itself by either a security or assurance lapse. Consider which other parties personal information is shared with, what reliance those parties have on the correctness and timeliness of the information shared, and the consequences on the organisation if the shared information fell short of the receiving parties' needs. Then consider which malicious groups might represent a threat, what in the personal information might be of any value to groups of potential wrongdoers, what benefits they might be able to obtain from the personal information, and then the harm that could be caused to the individual or organisation. Consider, where possible, the resultant harm if the data were combined with other data that might be known publicly or otherwise already available to the wrongdoer.

a) Harm to the organisation

The damage caused to the organisation by these types of privacy failure will derive from the repercussions on the organisation from the harm the organisation allowed to happen to others by its lapses in protection.

The privacy failure cost calculation sheet in Appendix E might be of use to help assess the costs, loss of revenue and effect on resilience.

i) Legitimate purposes

Other Party	Value (£)			
	Minimum	Average	Maximum	Confidence
Parties providing services to the organisation's customers/citizens/employees a) Under an established agreement or contract b) Ad-hoc with the express consent of the individual				
Parties for which the organisation provides services to the other's customers/citizens/employees				
Official bodies or public authorities				
Other bodies or agencies with which the organisation has an agreement to share information (e.g., credit reference agencies)				
Any other business partners with which information is shared				
Employees				

ii) Improper purposes

Threat Agent	Value (£)			
	Minimum	Average	Maximum	Confidence
Business partners				
Criminals Often bank and credit card details to perform financial fraud.				
Competitors Possibly linked to potential increased revenues.				
Disaffected employees				
Errant employees				
Gossipmongers Perhaps information relating to public figures, celebrities, high net worth individuals or friends and family.				
Hackers If not criminal, the value of demonstrating a problem to cause embarrassment to the organisation or individuals.				
Detractors Hostile pressure groups and others out to discredit or damage the organisation.				
Others				
Maximum of i and ii above				

b) Harm to the individual

The value of personal information from this perspective is set by the level of distress or harm a person could reasonably be caused by a privacy failure arising from assurance mistakes with shared personal information or the misuse or abuse of personal information by unauthorised parties. As discussed, this is the maximum level of harm that could reasonably be caused by a serious privacy failure, not the average level or the level a common failure might cause.

As before (in 'value to the individual'), the damage caused by these types of privacy failure can be thought of as the loss of some form of life asset (e.g. time, freedom, wealth, wellbeing), but this time as a result of the misuse or abuse of their information by unauthorised parties. This might include (note the difference in examples from above):

- Loss of free time (e.g., people having to put in the time and effort to defend themselves against the attacks of others)
- Loss of freedom (e.g. people no longer able to act as they wish due to the unwanted attention they now receive)
- Financial loss (e.g., financial fraud or the theft of belongings)
- Physical damage to property or their person (e.g. if someone intending harm were to find out a new address)

- Reputational damage (loss of trust by other people and organisations)
- Emotional stress (e.g. anxiety, fear arising from harassment)
- Embarrassment (and the difficulties this can cause for personal relationships and opportunities)
- Intrusion into their private lives

An example calculation is shown in Appendix D.

Calculation method	Value per Individual (£)			
	Minimum	Average	Maximum	Confidence
Damage caused to the individual by a privacy failure All the potential mental, physical and financial harms including the costs of returning to normal over the duration of the impact, calculated as a present value.				
Number of individuals				
Total value for all individuals				

c) Value of the information

The maximum of a) and b) above.

Maximum of above	
-------------------------	--

Example: Personal information value to an online account aggregation user

An online financial service provides a facility for subscribers to consolidate and manage their various bank, building society, insurance and investment account details from a single console. The company has 150,000 customers using account aggregation.

Damage caused to the individual by a privacy failure

The greatest harm to the individual is the loss of their account details and the misuse of those by an unauthorised party who perhaps sells them on at which point they are used for identity theft. Appendix D shows an average of about £700 per individual, giving a total of £105 million harm. The worst cases might cost over £3,000 to correct the damage caused, equating to a maximum of £450 million.

Conclusion

The value based on the value to other parties and the harm to the individual approach, is around £450m.

Societal value

This is the importance to the organisation of “doing the right thing” with regard to privacy, plus the importance of compliance with regulations and legislation.

The value of “doing the right thing” is the value of having an organisational culture in which the people on which the organisation relies (stakeholders, employees, citizens or customers) have a high degree of trust in the organisation’s good behaviour and repay that trust in their own positive behaviours towards the organisation. Each organisation will have to assess how its ability to achieve its mission and be successful depends on the attitudes of its public and the ways in which those attitudes might be expressed. This value could manifest itself, for example, in stakeholders supporting organisational propositions, employees accepting and supporting necessary change, and citizen and customer loyalty. It could be estimated, perhaps, by looking to the effort and cost the organisation expends on its privacy ethics.

The value to society of having organisations comply with established privacy norms is incredibly difficult to estimate other than, admittedly imperfectly, through the fines, penalties and other forms of burden imposed by mandating powers.

Calculation method	Value (£)			
	Minimum	Average	Maximum	Confidence
Cost of the organisation's own privacy ethics				
Manifestations of stakeholder support				
Manifestations of employee support				
Manifestations of citizen / customer support				
Financial penalties From the ICO or industry-specific regulators (the direct costs of dealing with failures appears elsewhere).				
Restrictions on operational freedom Limitations on operations; withdrawal of licence.				
Jail sentences Where these are a possibility for non-compliance.				
Maximum of above				

Example: Personal information value to a high street retailer from society's perspective

A major retailer has over 40 stores in prime high street or shopping centre locations.

Cost of the organisation's own privacy ethics

The retailer believes it is DPA compliant but does not have particular additional internal privacy mandates.

Manifestations of stakeholder support

The company has not found that its stakeholders have been particularly proactive in privacy concerns. It does not have corporate customers, but if this were to change, the valuation here might become significant. This method is therefore not considered appropriate.

Manifestations of employee support

Manifestation of employee support has been determined by determining the cost of the internal "Better Employees - Better Business" human resources initiative. The effects of privacy concerns have been estimated as at most 10% of the cost of this programme, or £600,000.

Manifestations of citizen / customer support

The retailer considers trust in its brand to be the most important aspect and, in the absence of other data, asked a marketing consultancy to determine the value of its brand in the UK. This was found to be £3 million. Whilst there are many other factors that can affect brand value, protection of privacy was seen as an important aspect, and the retailer judged this total value would be the appropriate figure to use.

Financial penalties

The financial penalties from a major privacy breach would be imposed by the ICO. If a fine were imposed, it is expected this could amount up to a maximum of £500,000.

Restrictions on operational freedom

There are no threats to operational freedom. This method is therefore not considered appropriate.

Jail sentences

There is currently no prospect of custodial penalties for the company's officers. This method is therefore not considered appropriate, but will have to be considered again in due course as the penalties are currently under review, are likely to increase, and custodial penalties could become possible.

Conclusion

The value of the information based on the societal value, is the highest of the above – manifestation of citizen/customer support i.e. £3 million.

Appendix D: Worked example of harm to an individual

Cost to a victim of a privacy failure

This example estimates the harm caused to a victim of online ID fraud where their identity has been comprehensively stolen. This calculation of harm is illustrative and should be used with caution – please see the discussion of the problems relating to “per record” values in Part 1 of this volume.

Description	Calculation	Notes
1 Average financial loss ⁴² Average stolen from UK victims of online ID fraud within the last 12 months	Per victim: £463	Data released September 2009
2a Time spent dealing with the incident ⁴³ Where an identity is comprehensively stolen, the time required by a UK victim to sort out their life and clear their name	Per victim: 3 to 48 hours	2007 data
2b (Least average) non-working time cost If all the time to deal with the incident was undertaken during non-working time	Time (from 2a): 3 hours Non-working market price ⁴⁴ : £4.50/hour Cost = 3x4.50 = £13.50	2002 prices
2c (Greatest average) working time cost If all the time to deal with the incident had to be taken as unpaid leave from work, based on average pay	Time (from 2a): 48 hours Mean gross earnings ⁴⁵ : £481/week Mean paid hours ⁴⁶ : 32.4 hours/week Income tax and NI (indicative) ⁴⁷ : 17% Cost = (48/32.4)x481x0.83 = £591.45	2009 data 2009 data 2003/04 data
3 Average financial and time loss	From 1, 2b and 2c (to nearest pound): Least average = 463+13 = £ 476 Greatest average = 463+591 = £1,054 Average range £450 to £1,050	Rounding to nearest £50

There is insufficient statistical data to determine the error ranges of these estimates.

42 One in Eight Brits Fall Victim to Online ID Fraud, Press Release about YouGov survey, Verisign 16 September 2009, http://www.verisign.co.uk/press/page_20090916.html

43 Identity Fraud and Identity Theft, CIFAS, 2008, http://www.cifas.org.uk/default.asp?edit_id=968-56

44 Department for Transport, <http://www.dft.gov.uk/pgr/economics/rdg/reportonworkshoptraveltimes1081?page=3>

45 All Employees, Table 1.1a, 2009 Annual Survey of Hours and Earnings, Office for National Statistics, <http://www.statistics.gov.uk/statBase/product.asp?vlnk=15313>

46 All Employees, Table 1.10a, 2009 Annual Survey of Hours and Earnings, Office for National Statistics, <http://www.statistics.gov.uk/statBase/product.asp?vlnk=15313>

47 Percentage of Earnings Paid in Income Tax and National Insurance Contributions: By Sex and Level of Earnings, Office for National Statistics, <http://www.statistics.gov.uk/StatBase/ssdataset.asp?vlnk=7434&Pos=1&ColRank=2&Rank=240>

A mid-range value, to the nearest £100, would be:

Typical value	At least £700
----------------------	----------------------

Amplifiers

The value (in this case the harm) to the individual would be uplifted by:

- Expenses for dealing with the incident (e.g. cost of postage, telephone calls, fees)
- Loss of entitlement to some other benefit
- Future, yet unknown, side-effects
- Emotional stress
- Loss of trust by other people and organisations
- Any potential physical or mental harm
- Increased risk of future harm
- Being part of a vulnerable group
- Updating the non-working cost data to current day values
- Higher than average earnings.

Attenuators

The value (in this case the harm) to the individual would be reduced by:

- Prevention of the privacy failure
- Compensation for the stolen money⁴⁸
- More rapid damage limitation and mitigation actions
- Lower than average earnings, or no loss of earnings incurred.

⁴⁸ A quarter of the victims claimed to still be in dispute over compensation for the money that was stolen from them, http://www.verisign.co.uk/press/page_20090916.html

Appendix E – Privacy failure costs calculation sheet

Here we provide a calculation sheet to help organisations estimate the direct costs they might experience due to privacy failures.

Before completing this calculation sheet, the reader is advised to review the discussion of the consequences of privacy failures presented in Part 1 of this document. In that section, consequences were described as being direct, indirect and wider. The costs calculated here are for the direct consequences of privacy failures. The other consequences are estimated in a different way in the next appendix, Appendix F (as a loss of benefits).

Privacy failures can take any of a wide variety of forms and not all of them involve the loss of personal data. Failures include contravention of any applicable privacy mandate, including any of the eight principles of the Data Protection Act. Thus not processing personal data fairly is a privacy failure too.

It is important that the full breadth of privacy failures is understood, not only for the purposes of this calculation sheet but also to ensure that the monitoring and reporting conducted within the organisation captures all types of privacy failure and does not become based solely around a limited range of failures such as security incidents where personal data losses have occurred. The organisation needs to include all types of failure within its reporting systems so it can understand where and how often each type occurs, enabling it to judge its full exposure to privacy failures.

The organisation can use this calculation sheet to quantify its own likely direct costs associated with different types of privacy failure. Some monetary values will have to be estimated, but the organisation will be able to judge these for itself based on its own sector and management information.

The types of failure that should be considered should be drawn from a risk assessment (incorporating privacy) or a privacy impact assessment⁴⁹ but might include:

- Using existing personal information for purposes other than originally intended
e.g. merging it with sensitive data from another source to make new business data
- Collection of excessive information
e.g. asking for a full postal address when the service requested does not involve delivery to a physical address and where the full address is not required to validate a transaction
- Not providing details of what information is held on an individual to the data subject themselves
e.g. not responding to a subject access request in the required time
- Inadequately secure disposal
e.g. sensitive data disposed of in standard rubbish bins, or confidential rubbish not properly protected before destruction, and acquired by, for example, an investigative journalist looking into how organisations continue to disregard privacy.

⁴⁹ Privacy Impact Assessment Handbook, Version 2.0 ICO,
http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/index.html

- Inadequate data security
e.g. a laptop stolen containing encrypted data about vulnerable children, but where the encryption password was stolen at the same time
- Data held in another country without adequate protection
e.g. a back-up copy of a website database containing all the organisation's customer data being used in another country for software testing purposes
- Automated decision making
e.g. credit worthiness decisions being made about individuals solely by automated processing

Most failures will not include all the damage items listed below. Some may include them all.

Where values are difficult to quantify, recent surveys may help with more general data⁵⁰ .

⁵⁰ 2009 Annual Survey: UK Cost of a Data Breach, PGP and the Ponemon Institute, January 2010, <http://www.encryptionreports.com/costofdatabreach.html#hgTab-2>

Direct Costs

Section	Item	Quantity	Unit	Rate (£)	Cost (£)
Response	Initial investigation and assessment		hours		
	Containment and mitigation (people from a number of areas might be involved)		hours		
	Forensic analysis including evidence collection and preservation		hours		
	Review and planning		hours		
	Identification of potential victims		hours		
	Assessment of risk to individuals		hours		
	Assessment of notification requirements (harm, scale and data sensitivity)		hours		
	Public relations (e.g. customers, investors)		hours		
	Crisis management		hours		
	External support services				
Notification	Preparation of notification and reporting materials		hours		
	Contacting potential victims (letters, telephone calls, emails and notices)				
	Information Commissioner's Office ⁵¹				
	Police and other law enforcement				
	Regulators				
Individuals	Support services (call centre contact, counselling, legal advice, advocacy)				
	Identity theft insurance				
	Financial (credit) monitoring				
	Identity theft monitoring				
	Restoration of damage				
	Recompense and remediation				

⁵¹ Notification of Data Security Breaches to the Information Commissioner's Office, ICO, 27 March 2008, http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/breach_reporting.pdf

Section	Item	Quantity	Unit	Rate (£)	Cost (£)
System or business process	Root cause analysis and remediation planning		hours		
	Labour to plan, acquire and implement preventative measures (multiple information systems might need to be patched or upgraded)		hours		
	Additional services and materials				
	Additional employee education		hours		
	Management		hours		
Business	Legal costs				
	Regulator's charges and investigation fees				
	Own costs supporting external investigations				
	Issue of new accounts, paperwork, cards, credentials				
	Fines from regulators				
	Costs of other penalties imposed by regulators (e.g. investigation fees)				
	Fines from courts				
	Disruption to normal operations over the entire duration of containment activities				
	Increased operating costs (e.g. transaction fees)				
	Increased employee training costs				
	Increased management costs				

Appendix F – Privacy protection benefits calculation sheet

Here we provide a calculation sheet to help organisations estimate the magnitude of the benefits they might expect to see.

Before completing this calculation sheet, the reader is advised to review the discussion of the consequences of privacy failures and the benefits of privacy protection presented in Part 1 of this document.

The organisation can quantify its expected benefits by considering how better privacy protection might help the organisation achieve its business objectives. We develop the calculation sheet here for the five business objectives considered common to most if not all organisations (increase resilience, increase returns, reduce operating costs, reduce risks, improve compliance). Each organisation can extend the sheet to include its other business objectives.

As before, the organisation should consider all types of personal information it processes and each group of people on which it relies (e.g. stakeholders, employees, citizens, customers).

Increase resilience

The effect on resilience is associated with the depth of trust held by the organisation's public. It might be measurable by assessment of brand value or even equity value. Enter into the table below those factors that are thought to affect resilience for the organisation, how better privacy protection might influence these, and quantify the benefit as much as possible. Research on the economics of privacy may provide useful guidance^{52 53}.

Factor	Effect	Benefit (£)

Increase returns

The nature of these returns will vary depending on the sector the organisation is in, the group of people considered and the way their personal information is used. It can include sales income, value of contracts, service take-up. It can also include the strengthening of strategic decisions made on the basis of more complete, accurate or relevant personal information held.

Factor	Effect	Benefit (£)
Increased take up of services		
Increased coverage of specified citizen groups		
Increased sales volumes (number		

52 The Economics of Privacy, Alessandro Acquisti, <http://www.heinz.cmu.edu/~acquisti/economics-privacy.htm>

53 Economics of Privacy, Economics and Security Resource Page, Ross Anderson, <http://www.cl.cam.ac.uk/~rja14/econsec.html#Privacy>

Factor	Effect	Benefit (£)
of customers and sales per customer)		
Increased premium charged on offerings		
Increased customer loyalty		
Increased market penetration		
Increased differentiation		
Increased average donation size or frequency		
Increased number of donors		
Increased business opportunity		
Reduced time to market		

Reduce operating costs

These are of two types. The most obvious is the reduced direct costs of dealing with privacy failures owing to the reduced likelihood that such failures will occur. These costs can be estimated using the calculation sheet in Appendix E. Better protection of privacy can also reduce business-as-usual operating costs in a number of ways. These will normally be very specific to the organisation and group of people, and, as a result, many of the areas mentioned below might not apply.

Factor	Effect	Benefit (£)
Reduced cost of acquiring customers, participants, etc.		
Reduced customer management costs (e.g. letters written, requests having to be made, calls received, questions to be answered, complaints handled)		
Reduced cost of customer retention incentives		
Reduced costs of employee churn (recruitment and training)		
Reduced costs of attracting and retaining high-skill or in-demand specialised employees		
Reduced employee management costs (e.g., better quality of information)		
Reduced costs of managing		

Factor	Effect	Benefit (£)
outsourced service providers (where the provider is handling the organisations' information)		

Reduce risks

The reduction in security risks arises from the reduced likelihood that such security failures will occur. The costs associated with these can be estimated using the calculation sheet in Appendix E. Better protection of privacy can also reduce other aspects of risk. These will be organisation-specific and taken from the organisation's risk register.

Type	Description	Previous Residual Risk Level	Influence of privacy improvement	New Residual Risk Level
Operational				
Strategic				
Project				
Market				
Compliance	See below	-	-	-

Compliance

The particular compliance requirements will vary with organisation. Even the number of regulators will vary and could be in the hundreds, but the number of mandates where a privacy failure could lead to non-compliance will be fewer. The organisation should identify the relevant mandates, identify

the aspects that relate to privacy protection, the risk of non-compliance (unintentional or otherwise) and the impact of non-compliance (fines, penalties, operational and strategic impact). Lists of legislation and other areas of law in the ICO PIA Handbook⁵⁴ may also be of use.

Section	Description	Issues
Internal	Policies	
	Contracts	
External	UK Data Protection Act 1998 (DPA)	
	UK Privacy and Electronic Communications Regulations 2003 (PECR)	
	EU Directive 95/46/EC (Data Protection)	
	EU Directive 2006/24/EC (Data Retention)	

⁵⁴ Privacy Impact Assessment Handbook, Version 2.0 ICO,
http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/index.html
http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/html/2-Chap6b.html
http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/html/3-app1.html#step3

Appendix G - Mandates for privacy protection

The ICO⁵⁵ is the sole regulatory body for data protection in the UK and publishes extensive guidance for organisations⁵⁶.

Note: Scotland has its own Information Commissioner⁵⁷ who regulates the Freedom of Information (Scotland) Act which covers Scottish public authorities.

Worksheet

Review the mandates for privacy protection in the organisation using the following table as an initial guide. Speak with employees from all parts of the organisation to identify mandates they are aware of and check the list of bodies below for further ideas. Also refer to the information on compliance checking in ICO PIA Handbook⁵⁸.

Type	Name	Applicable	Notes
Corporate	Strategic objectives		
	Statutory obligations		
	Policies (e.g. privacy, security, ethical)		
	Internal standards		
	Contractual requirements (suppliers, customers, insurers, advisors, employee representatives, and with the public)		
	Service agreements		
	Performance indicators		
	Business change programmes		
	Initiatives		
	Business "trust seal" or "privacy seal" programmes and guarantees		
	Employee agreements		
External standards	BS 10012:2009		
	ISO/IEC 27000 series		

55 <http://www.ico.gov.uk>

56 Data Protection Guide for Organisations http://www.ico.gov.uk/for_organisations/data_protection_guide.aspx

57 <http://www.itpublicknowledge.info>

58 Privacy Impact Assessment Handbook, Version 2.0 ICO, http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/index.html

Type	Name	Applicable	Notes
Other (see also Employee Professional Associations and Unions and International Aspects, and Other Initiatives below)			

List of external bodies

This section is a non-exhaustive list of common UK regulators, trade organisations and associations that compel or recommend compliance with the Data Protection Act 1998, or impose additional or more specific privacy protection measures and which are detailed in their guidance notes, codes of practice and other publications.

Some organisations can have hundreds of regulators, including some located in other countries. A full list⁵⁹ of UK regulators is maintained by the Cabinet Office, (see Public Bodies 2008⁶⁰ for all regulatory bodies and a convenient, albeit out-of-date, summary in Appendix 2 of Public Bodies 2006⁶¹).

Many bodies have multiple documents with requirements and guidance, and in these cases, only the most significant ones are listed. Check for the latest versions of each document listed, and any additional related requirements and guidance.

See also the codes of practice produced by the ICO in consultation with trade associations and consumer or representative groups⁶².

- Advertising Standards Authority
 - British Code of Advertising, Sales Promotion and Direct Marketing
http://www.asa.org.uk/asa/codes/cap_code/CodeIndex.htm
- Association of British Insurers (ABI)
 - Guidelines on the instruction and use of private investigators and tracing agents, July 2007
<http://www.abi.org.uk/content/contentfilemanager.aspx?contentid=24973>
- Association of the British Pharmaceutical Industry
 - Publications
<http://www.abpi.org.uk/publications>
- Audit Commission for Local Authorities in England and Wales

59 <http://www.civilservice.gov.uk/about/work/codes/public-bodies.aspx>

60 http://www.civilservice.gov.uk/Assets/PublicBodies2008_tcm6-6429.pdf

61 http://www.civilservice.gov.uk/Assets/publicbodies2006_tcm6-2474.pdf

62 http://www.ico.gov.uk/Home/what_we_cover/data_protection/guidance/codes_of_practice.aspx

- Code of Data Matching Practice
<http://www.audit-commission.gov.uk/localgov/audit/nfi/Pages/code.aspx>
- KLOE 8 - Reliable Data and Information
<http://www.audit-commission.gov.uk/localgov/audit/childrenandyoungpeople/lactoolkit/pages/kloe8.aspx>
- Audit Scotland
 - Code of Data Matching
http://www.audit-scotland.gov.uk/docs/central/2006/nr_060712_nfi_data_matching_practice.pdf
 - Publications
<http://www.audit-scotland.gov.uk/about/as/docs.php>
- BBC
 - Editorial Guidelines
<http://www.bbc.co.uk/guidelines/editorialguidelines/edguide/>
 - Online Services Guidelines
<http://www.bbc.co.uk/guidelines/editorialguidelines/assets/onlineservices/osg.pdf>
- Becta
 - Data Handling Security Guidance for Schools
http://schools.becta.org.uk/index.php?section=lv&catcode=ss_lv_mis_im03&rid=14734
 - Data Protection and Freedom of Information in Schools
http://schools.becta.org.uk/index.php?section=lv&catcode=ss_lv_mis_im03&rid=629
- British Bankers' Association
 - Keeping customer information safe, July 2007
http://www.bba.org.uk/content/1/c6/01/10/10/Keeping_Customer_information_safe_2007.pdf
- British Parking Association
 - Code of Practice
 - Code of Professional Conduct
http://www.britishparking.co.uk/includes/tiny_mce/jscripts/tiny_mce/plugins/filemanager/files/join/code_of_professional_conduct_jan05.pdf
- Cabinet Office
 - Data Handling Procedures in Government
http://www.cabinetoffice.gov.uk/reports/data_handling.aspx
 - HMG Security Policy Framework
<http://www.cabinetoffice.gov.uk/spf.aspx>
- Care Quality Commission
 - The Right Information, in the Right Place, at the Right Time
http://www.cqc.org.uk/_db/_documents/Info_governance_FINAL_PDF.pdf
- Charity Commission
 - Open Government and Human Rights
<http://www.charity-commission.gov.uk/supportingcharities/opengov.asp>
 - Reporting Serious Incidents
<http://www.charity-commission.gov.uk/investigations/rsi.asp>

- Risk and Proportionality Framework for the Commission's Compliance Work
<http://www.charity-commission.gov.uk/investigations/riskprop.asp>
- Consumer Credit Association
 - Code of Practice
<http://www.ccauk.org/downloads/CodeOfPractice.doc>
 - A Guide to the Use of Your Personal Data By Consumer Credit Association Members and Credit Reference and Fraud Prevention Agencies
<http://www.ccauk.org/downloads/DPGuide.pdf>
- Consumer Credit Trade Association
 - Code of Practice
<http://www.ccta.co.uk/CodeOfPractice.pdf>
 - Code of Practice for Driver and Vehicle Licensing Agency (DVLA) Keeper Data Access
<http://www.ccta.co.uk/CodeOfPracticeDV.pdf>
- Credit Services Association
 - Code of Practice
<http://www.csa-uk.com/page/codes-and-standards>
- Criminal Records Bureau
 - Handling of Disclosure Information
http://www.crb.gov.uk/guidance/rb_guidance/handling_of_disclosure_info.aspx
- Department for Business, Innovation and Skills
 - Statutory Code of Practice for Regulators
<http://www.berr.gov.uk/files/file45019.pdf>
- Department for Children, Schools and Families
 - Safeguarding Children and Safer Recruitment in Education
<http://publications.teachernet.gov.uk/eOrderingDownload/Final%206836-SafeGuard.Chd%20bkmk.pdf>
- Department of Health
 - Information Governance
<http://www.dh.gov.uk/en/Managingyourorganisation/Informationpolicy/Informationgovernance/index.htm>
 - Information Governance Toolkit
<https://www.igt.connectingforhealth.nhs.uk/>
 - NHS Codes of Practice and Legal Obligations
<http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/codes>
 - Patient Confidentiality and Access to Health Records
<http://www.dh.gov.uk/en/Managingyourorganisation/Informationpolicy/Patientconfidentialityandcaldicottguardians/index.htm>
 - Records Management and Data Quality
<http://www.dh.gov.uk/en/Managingyourorganisation/Informationpolicy/Dataquality/index.htm>
- Direct Marketing Association
 - Code of Practice
<http://www.dma.org.uk/membership/mem-code.asp>

- Best Practice Guidelines
<http://www.dma.org.uk/information/inf-practice.asp>
- Finance and Leasing Association
 - Guidance
- Financial Services Authority
 - Banking Conduct of Business Sourcebook
<http://www.fsa.gov.uk/Pages/Doing/Regulated/bcoobs/>
 - Data Security in Financial Services
http://www.fsa.gov.uk/pubs/other/data_security.pdf
 - Handbook
<http://www.fsa.gov.uk/Pages/handbook/>
 - Publications for consumers
<http://www.moneymadeclear.fsa.gov.uk/publications>
- General Medical Council
 - Confidentiality: Protecting and Providing Information (Ethical Guidance)
<http://www.gmc-uk.org/guidance/current/library/confidentiality.asp>
 - Management for Doctors
http://www.gmc-uk.org/guidance/current/library/management_for_doctors.asp
 - Research: The Role and Responsibilities of Doctors
<http://www.gmc-uk.org/guidance/current/library/research.asp>
- Health Protection Agency
 - Safeguarding the Confidentiality of Patient Information While Also Protecting Public Health
http://www.hpa.org.uk/webc/HPAwebFile/HPAweb_C/1194947352367
- Learning and Skills Council
 - Data Protection
<http://www.lsc.gov.uk/providers/Data/help/dataprotection/>
- Medicines and Healthcare products Regulatory Agency
 - Publications
<http://www.mhra.gov.uk/Publications>
- Healthcare Inspectorate Wales
 - Publications
<http://www.hiwi.org.uk/page.cfm?orgid=477&pid=13323>
- Home Office
 - Code of Practice on Data Retention
<http://www.opsi.gov.uk/si/si2003/draft/5b.pdf>
- Information Commissioner's Office
 - Codes of Practice
http://www.ico.gov.uk/Home/what_we_cover/data_protection/guidance/codes_of_practice.aspx
 - For organisations
http://www.ico.gov.uk/for_organisations.aspx
- Internet Advertising Bureau

- Good Practice Principles for Online Behavioural Advertising
<http://youronlinechoices.co.uk/wp-content/uploads/2009/09/IAB-Good-Practice-Principles-for-Online-Behavioural-Advertising.pdf>
- Online Guides
<http://www.iabuk.net/en/1/internetmarketingguides.html>
- JANET
 - Policies and Legal Requirements
<http://www.janet.ac.uk/services/publications/supportmanual/policies.htm>
 - Suggested Charter for Systems Administrators
<http://www.janet.ac.uk/development/legal-and-regulatory/regulated-activities/charter-for-system-administrators.html>
 - Logfiles (UKERNA Technical Guides)
<http://www.janet.ac.uk/documents/publications/technical-guides/logfiles.pdf>
- Joint Information Systems Committee
 - Code of Practice for the Further and Higher Education Sectors on the Data Protection Act 1998
<http://www.jisclegal.ac.uk/Portals/12/Documents/PDFs/DPACodeofpractice.pdf>
- The Law Society
 - Data Protection Practice Note
<http://www.lawsociety.org.uk/productsandservices/practicenotes/dataprotection/2223.article>
- The Law Society of Scotland
 - Confidentiality (Advice Rules and Guidance)
[http://www.lawscot.org.uk/Members Information/rules and guidance/guides/Rules/Confidentiality/confidential.aspx](http://www.lawscot.org.uk/Members%20Information/rules_and_guidance/guides/Rules/Confidentiality/confidential.aspx)
- Local Government Association
 - Data Handling Guidelines
<http://www.lga.gov.uk/lga/aio/1587602>
- London Internet Exchange
 - Memorandum of Understanding
<https://www.linx.net/govern/mou.html#confidentiality>
 - Traceability (Best Practice)
https://www.linx.net/good/bcp/traceability-bcp-v1_0.html
- Medical Research Council
 - Data Access (Research Guidance)
<http://www.mrc.ac.uk/Ourresearch/Ethicsresearchguidance/Dataaccess/index.htm>
 - Data Sharing Initiative (Research Guidance)
<http://www.mrc.ac.uk/Ourresearch/Ethicsresearchguidance/Datasharinginitiative/index.htm>
 - Guidelines for Good Clinical Practice in Clinical Trials
<http://www.mrc.ac.uk/Utilities/Documentrecord/index.htm?d=MRC002416>
- National Association for Voluntary and Community Action
 - Policies and procedures
<http://www.navca.org.uk/about/navcapolicy/>

- National Health Service
 - Codes of Practice and Legal Obligations (see Department of Health)
- The National Council for Voluntary Organisations
 - Data Protection Law
<http://www.ncvo-vol.org.uk/askncvo/index.asp?id=14918>
- National Information Governance Board for Health and Social Care
 - Care Record Guarantee
<http://www.nigb.nhs.uk/guarantee>
 - Information About Patients (Patient Information Advisory Group)
<http://www.advisorybodies.doh.gov.uk/piag/InformationAboutPatients.pdf>
- National Patient Safety Agency
 - Protecting the Anonymity of Information Providers
<http://www.ncas.npsa.nhs.uk/EasySiteWeb/GatewayLink.aspx?allid=9624>
 - Security of NHS patient data shared for research purposes
<http://www.nres.npsa.nhs.uk/EasySiteWeb/GatewayLink.aspx?allid=18081>
- National Union of Journalists
 - Code of Conduct
<http://www.nuj.org.uk/innerPagenuj.html?docid=174>
- Northern Ireland Audit Office
 - Code of Conduct
http://www.niauditoffice.gov.uk/pubs/NIAO_Code_of_Conduct.pdf
 - Code of Data Matching Practice
<http://www.niauditoffice.gov.uk/pubs/nfi/consultationCode/CodeOfDataMatchingPractice.pdf>
- Northern Ireland Council for Voluntary Action
 - Good Practice Guides
<http://www.nicva.org/index.cfm/section/article/page/NICVAGoodPracticeGuides>
- Office of Fair Trading
 - Advice and resources
http://www.oft.gov.uk/advice_and_resources/
- Office of the Scottish Charity Registrar
 - Guidance for Charity Trustees
<http://www.oscr.org.uk/DocumentViewer.aspx?ID=1b4ac026-b2e7-42a6-beb4-7aef0e6a6379>
- Ofcom
 - Letter of Understanding between the Office of Communications and the Information Commissioner's Office
<http://www.ofcom.org.uk/about/accoun/ico/>
- PhonePayPlus
 - Code of Practice
<http://www.phonepayplus.org.uk/output/Code-of-Practice-1.aspx>
- Press Complaints Commission

- Code of Practice
<http://www.pcc.org.uk/cop/practice.html>
- Data Protection Act, Journalism and the PCC Code
<http://www.pcc.org.uk/news/index.html?article=ODg=>
- Editors' Code of Practice
http://www.pcc.org.uk/assets/111/Code_Aug_2007.pdf
- The Property Ombudsman
 - Code of Practice for Residential Estate Agents
http://www.tpos.co.uk/downloads/IES02_code%20of%20practice_sales.pdf
- Scottish Commission for the Regulation of Care
 - Publications
http://www.carecommission.com/index.php?option=com_content&task=view&id=44&Itemid=73
- Scottish Council for Voluntary Organisations
 - Information
<http://www.scvo.org.uk/scvo/Information/Information.aspx>
- The Scottish Government
 - Data Handling in Government
<http://www.scotland.gov.uk/Resource/Doc/229747/0062215.pdf>
- Society of Editors
 - Code of Practice
http://www.societyofeditors.co.uk/page-view.php?page_id=194&parent_page_id=140
- Society of Local Authority Chief Executives and Senior Mangers
 - Data Handling Guidelines (see Local Government Association)
- Solicitors Regulation Authority
 - Solicitors' Code of Conduct
<http://www.sra.org.uk/solicitors/code-of-conduct.page>
- Tenant Services Authority
 - Good Practice
<http://www.tenantservicesauthority.org/server/show/nav.13746>
- UK Payments Administration
 - Publications
http://www.ukpayments.org.uk/resources_publications/
- UK Research Integrity Office
 - Code of Practice for Research
http://www.ukrio.org.uk/sites/ukrio2/the_programme_of_work/code_of_practice_for_research.cfm
- Wales Council for Voluntary Action
 - Policy and research
http://www.wcva.org.uk/policy/index.cfm?display_sitedeptid=9&display_sitetextid=96
- Welsh Assembly Government

- Code of Practice on Access to Information
<http://new.wales.gov.uk/cisd/publications/codeaccessinfo2007/codee.pdf?lang=cy>
- Welsh Local Government Association
 - Data Handling Guidelines (see Local Government Association)

Employee professional associations and unions

Organisation employees are often members of their own professional, employee and interest groups. These groups often have their own codes of conduct, ethics, good practice, etc and may also stipulate compliance with legislation as being a condition of membership.

Although they are not corporate mandates, these aspects may have to be considered in particular business processes, teams or locations.

International aspects

For organisations with operations in another country, or where the parent organisation is located abroad, additional mandates may apply.

Employees in subsidiaries in other countries may be used to more strict, or less strict, privacy protection requirements or social norms.

Other initiatives

Many international bodies, open communities and major IT vendors are responding with privacy frameworks, guidelines, codes of practice and other initiatives.

Initiatives are changing all the time and new ones are being developed. A short illustrative list of some of these is provided below, but organisations should enquire about the most relevant current ones amongst the bodies and vendors they favour working with.

- European Commission
 - Think Trust
<http://www.think-trust.eu/>
 - Data Protection
http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm
- Future of Identity in the Information Society
 - Resources
<http://www.fidis.net/resources/>
- The Liberty Alliance
 - Strategic Initiatives
http://www.projectliberty.org/liberty/strategic_initiatives
- Online Privacy Alliance
 - Privacy Resources for Businesses
<http://www.privacyalliance.org/businesses/>
- Organisation for Economic Co-operation and Development
 - Information Security and Privacy
http://www.oecd.org/department/0,3355,en_2649_34255_1_1_1_1_1,00.html