Results from the People-Centric Information Assurance Workshop of 18 August 2009

Introduction

People, data subjects, understand that organisations need access to their personal information if those organisations are to deliver more personalised and more convenient services. Generally, people do not object to providing personal information if it is relevant to the services they want to access. However, there are limits to what people are prepared to accept. Given there are these limits, processors of personal information, whether from the public or private sector, need to understand and stay within these limits if they are not to alienate people and lose the goodwill and trust of their citizens or customers. IAAC's objective for this workshop, the third in its PCIA series, was to provide guidance for information processors on how to stay within these limits, acquiring and using personal information whilst maintaining respect for people's sensitivities and the limits of their tolerance.

This report is not intended to serve as a record of the workshop discussion. It is, as with previous workshop reports, a digest of many of the insightful points made during the discussion.

Disclaimer: The ideas expressed in this paper should not be taken to represent the views of any individual IAAC member or sponsor.

Key Messages

1. People realise that digital systems are not perfect. Harms can arise unintentionally either because of a shortcoming in the way the system was designed or a shortcoming in the way it is used. This is the case for both public and private sector personal information systems.
2. Privacy is a long-standing right and has been the mainstay of people's protection against possible harms, in part because of its ability to provide protection across a wide range of situations, usual and unusual. However, personal privacy is now being eroded as personal information systems encroach more and more into people's lives.
3. An erosion of privacy does not have to mean an erosion of protection. What has in the past been articulated as the Right to Privacy should perhaps be seen for what it is, a Right to Protection. If privacy is being eroded, then clearly other safeguards (e.g., transparency, accountability, auditability, reporting) should be stepped up to take the strain. People have a right to protection and should not have to settle for less.
4. If protection is to continue to be provided across a widely diverse range of situations, organisations need to root their approach to protection in the development of a people-centric corporate culture and value system. Simply providing a wider range of privacy options within the services the organisation offers will not be sufficient to cope with the diversity of people's needs. Adopting a more people-centric culture will not only help organisations to cause less harm, it will encourage people to trust them more and that will be in the organisation's better interests.
5. Organisations need to improve the way that personal information systems are designed so systems reflect better the way people deal with relevant personal issues and the many different ways systems will get used. System designers should adopt a more people-centric view of a system's purpose and what the public will want from the system, not stick with the traditional organisation-centric view.
6. Having the data subject's consent should not be seen as a silver bullet, obtained once to allow any and all subsequent data sharing and use. Information use still has to be fair, appropriate to the stated purpose, and limited to the context under which consent was granted.

Registered Number 432637
Sponsors:

Discussion

The Shifting Landscape

The preceding two workshops provided opportunities for delegates to discuss the ways in which the landscape of society and the fabric of people's lives are changing as the UK becomes increasingly digital. To those findings can be added:

1. Somewhat in contrast with other EU member states, the UK's path to being a digital society has led to the development of large intrusive IT systems. Some are centralised (e.g. the National DNA Database; the National Identity Register), others are not (e.g. CCTV). These give the appearance that the balance of government systems has shifted, incrementally, to emphasise less serving the interests of the individual and more serving the interests of the state.

2. Incremental steps can, over time, lead to a significant change in culture. It is not safe to presume that change achieved in this way is always change that people would welcome. People might not wish for such change, or might prefer if it took alternative forms.

People's Responses to These Shifts

Likewise the preceding workshops provided opportunities for delegates to discuss the ways in which people's attitudes are changing as a result. To those findings can be added:

3. As people become more aware of the encroachment of digital systems into their lives, they become more alert to the risks associated with the processing of their personal information and more aware that they need to take care. They are becoming less trusting, more cautious and more possessive of their personal information. They apply tactical steps to defend themselves when they feel they might be particularly vulnerable.

4. People's attitudes towards digital technologies are very particular and vary from individual to individual. Some people feel more vulnerable in the presence of digital systems than others. Many people in the UK see static-camera CCTV as being benign and a source of reassurance, not solely as an intrusive technology. Moving-camera CCTV, though, is seen as less benign; it triggers a fear of predation in some women. For some people, their sense of freedom and autonomy is not much constrained by the presence of CCTV. For others, it is.

5. The National DNA Database tends to cause people considerable levels of concern. This is perhaps because people feel that DNA profile data, even though it is profile data rather than actual DNA data, can be used in potentially powerful ways that can have very significant impacts on people. These uses could cause an innocent person enormous distress and disadvantage and leave them with no easy way to unravel a situation that has arisen in error or undo the harm they have wrongly been caused.

6. In addition to harms that can be inflicted on individuals, people have concerns regarding the possible harm that can be caused to societal values. There is societal value in the protection of privacy, not just value to the individual. Would we want ours to be a society in which everyone had volunteered to give up their privacy? Privacy is important for autonomy, dignity, independence, and for strengthening social and political relations, not just for enabling us each to stand aloof from others.

7. The National DNA Database appears to some to reverse the presumption of innocence. This is seen as a violation of a principle which has long been afforded a very high societal value.

The Source of These Concerns

Why is it that people feel digital systems make them more vulnerable?

8. One reason some people feel concerned about the encroachment of digital systems is that they realise digital systems and the way their outputs are used are not always flawless. There will always be situations in

which unintended consequences arise. These unintended consequences can be particularly damaging when the digital systems are government systems that exert influence or control over people.

9. For example, consider government data gathering and data sharing systems. These are not intrinsically evil, they have arisen because of the benefits they bring (to individual people or to society). People and organisations have shared information for duty-of-care reasons for many years. Digital systems simply bring greater capacity. They enable more information to be shared, for sharing to be performed more widely, and for sharing to be performed for a greater number of purposes. This greater capacity multiplies the opportunities for things to go wrong, and for harms to be caused (to individuals or to society) whether by mistake or otherwise.

10. There are three general purposes for which government gathers and shares personal information: service delivery; protecting citizens; administration. Where people are concerned that government systems make them feel vulnerable, they are likely to be concerned predominantly with information being gathered for protection purposes rather than its being gathered for service delivery or administration purposes.

11. Harms can arise when digital systems make mistakes, i.e. when their design does not cater sufficiently well for all of the less common situations that might arise. But harms can also arise when the people working with those systems make mistakes. People working with government systems (e.g. lower ranks of the Civil Service) are, by reputation, often thought to be demotivated, and demotivated staff are more prone to errors.

12. The potential for harms to arise is not unique to Government systems. Just as there are weaknesses associated with Government practices there are weaknesses associated with private sector practices. It is, perhaps, a moot point which are likely to cause most harm. It becomes, instead, a question of trust. Some people might prefer to have their personal information held by Government, others by the private sector (e.g., Microsoft or Google), and yet others perhaps by a body somewhere in between (e.g., the Post Office).

The Need for Safeguards

It is this potential for personal information systems to cause harms, even if those harms are unintentional, that leads to protections and safeguards being needed.

13. Protections and safeguards exists to protect people's interests whenever personal information is shared or used. A right to privacy is one such protection. Historically, a right to privacy has been one of the more universal and long-standing protections people have been afforded in Western democracies.

14. Privacy is a fundamental right but it is not an absolute right. In particular situations, it is proper that an individual's privacy can be overridden in favour of other interests (e.g. investigation of crime, national security). This has long been the case and is not new or particularly different for digital systems. It is perhaps just that the power of contemporary digital systems has bought this issue more to the fore.

15. However, that does not mean that there should be no safeguards applying when the individual's interests take second place and their privacy is overruled. Rather, that different safeguards should apply, safeguards that cater for these situations.

16. Most safeguards will relate to 'normal practice', whether that be normal practice in situations where the individual's interests take precedence or normal practice in situations where the individual's interests take second place. However, provision is also needed for the uncommon, unusual or unique situations that fall outside normal practice. In those situations, normal safeguards might need to be set aside. However, again, that does not mean that there should be no safeguards applying in those cases, rather that the safeguards applied might need again to be different, and in force only temporarily whilst the unusual situation persists.

17. Privacy as a principle has the flexibility to serve well as a protection across a wide range of situations, usual and unusual. Some people feel, though, that, save for the right to privacy, the other safeguards that should be protecting people's interests are either missing or weak.

18. To that concern we can now add the perception that, as UK society becomes more digital, people's privacy, the central mainstay of the present protections, is itself being eroded. However, an erosion of privacy does not have to mean an erosion of protection. What has in the past been articulated as the Right to Privacy, a right enshrined in internationally accepted conventions, should perhaps be seen for what it is, a Right to Protection. If privacy is being eroded, then other safeguards (e.g., transparency, accountability, auditability, reporting) should be stepped up to take the strain. People have a right to protection and should not have to settle for less.

The Significance of Culture

19. Protections and safeguards exist to protect people and society against the harms that can arise from the things information processing organisations might do with personal information. They aim to constrain organisations' behaviours and prevent actions that might impinge adversely on people's or society's interests.

20. Ultimately, the things any information processing organisation does are decided upon and carried out by ordinary people, the organisation's staff. These ordinary people, to the extent that they too value the protection provided by privacy, might be expected to constrain for themselves and without the need for externally imposed controls, the actions they perform in the organisation's name. So why does this not ensure that no harm is ever done?

21. The way people do the things they do reflects the culture under which they act. Organisations each have their own culture, and that culture can be different from the culture that pertains outside the organisation and in people's homes. An organisation's culture also influences the encouragements and incentives it provides to its staff. Hence, people can behave differently as staff at work than they might as private individuals at home. They are capable of doing things at work that might be against people's private interests that they would not do if in the home. It is the organisation's culture that determines how staff behave, and if the organisation's culture is at variance with the culture in the communities around it, the organisation must bear responsibility for the resulting wrongs or harm their staff might cause.

22. A culture incorporates a value system. A value system is a shared acceptance of the relative importance of things considered worth protecting. Hence, an organisation's culture shows the importance the organisation gives to protecting privacy and what it considers important about the way it relates to the people it affects (citizens/consumers/staff). An organisation's culture also influences how the organisation governs its behaviour (e.g., the organisation's attitude towards accountability, authority, responsibility and transparency) and, in particular, how it governs its use of personal information.

23. A community's culture also incorporates a value system. Trust is based on sharing a value system. I.e., one person trusts another, or trusts an organisation, because he or she believes they share a value system. The person has confidence that the other party, whether a person or organisation, will decide and act as they would decide and act.

24. Hence, an organisation's culture not only affects how it relates to people and how it governs its use of personal information but also influences the trust people have in the organisation, and therefore how people behave when they relate to the organisation.

25. Safeguards serve to constrain the organisation's behaviours and limit the organisation's actions. Ideally, one effect of the weight of imposed safeguards would be to align the culture and value system of the organisation with the mainstream cultures and value systems that pertain in the society within which the organisation acts. To the degree that an organisation's culture and value system is so aligned, the safeguards imposed upon it become less a burdensome straightjacket on its operations and more a reflection of behaviours the organisation already seeks for itself.

The Place to Start

26. If protection is to continue to be provided across a widely diverse range of situations, information processors should start by looking to their culture, as it is their culture and the value system that underpins

it that guide, across all situations, usual and unusual, the way they handle people's personal information and the way they govern their own actions. Organisations that process personal information should strive to make their culture people-centric and ensure they acknowledge, respect and protect the interests of the people they affect across all the things they do.

27. Being people-centric should not be approached as simply another consumer issue to be addressed by providing a wider range of privacy options within the services the organisation offers. Simply providing additional options will not be sufficient to cope with the diversity of people's needs. It requires the organisation to acknowledge the power it has to affect people's lives, and to respect and take responsibility for the individual's concerns, interests, needs and rights.

28. It is not easy to develop policy and behaviours catering for the diversity of the public and the public's needs. For example, for each situation where it is natural to want to restrict the sharing of information, there will be some situations where it will be appropriate to overrule those restrictions, for example providing 3rd party access to a person's financial information when that person has died. There is a wide range of diverse situations such as these that have to be catered for. Because of the need to cater for this diversity, the place to start is to make the organisation's culture people-centric rather than simply to try to make each individual touch-point more flexible or allow more options.

29. Strengthening an organisation's culture is a huge challenge to undertake. However, it does provide returns. The organisation's culture and value system influence the way the organisation is seen by the people it affects and whether or not those people will trust the organisation. If the organisation respects the individual and works in line with their concerns, people will provide their trust, tolerance and cooperation in return. These all work to the organisation's benefit.

Governing Behaviour

30. The primary reason for developing a people-centric culture is for the organisation to govern its behaviours and actions with personal information in ways that respect people's concerns, interests, needs and rights. Hence, one of the first steps for the organisation should be to set out a governance approach under which it will constrain and govern its personal information behaviours.

31. Governing personal information behaviours is not just a technical matter requiring technical measures. As Principle 7 of the UK Data Protection Act states, appropriate technical and organisational measures are required.

32. Also, protecting personal information is not just about the protection of PII (Personally Identifiable Information – information that directly identifies a person). Aggregation and mining enables the effective identification of people without reliance on PII. Personal information includes any information that relates to an individual person, whether or not it is unique to that person, and it all needs to be protected.

33. Organisation's should look to align their behaviours with both internal and external mandates:
    - The DPA and its principles
    - Human rights
    - Applicable information handling guidance (regarding encryption, training, testing, and so forth)
    - Building privacy in to systems by design, following an organic design approach that includes PIAs
    - Strong and visible accountability throughout including at board level
    - Transparency built on strong reporting and scrutiny

34. The media has a powerful position in Western societies, and one part of its role is to be an advocate for the public interest. However, with power comes responsibility, including responsibilities relating to the way the media uses the personal information of public figures. These responsibilities need to balance the media's commercial imperatives of maximising circulation and profit.

The Design of Personal Information Systems

35. Conventionally, information systems are built under the presumption that users approach issues in the same way that the organisation approaches issues. For an organisation's internal management or administrative systems this might still be appropriate. But for systems facing the public and designed to meet the public's individual needs, this presumption is no longer safe, especially as people grow more used to Web 2.0 types of system. Organisations should adjust to a more people-oriented, less organisation-centric approach to designing public-facing information systems.

36. For example, they should not presume they know what people know, think or expect. The public have widely different exposures to ICT and take widely different positions regarding significant issues. It is best to validate what the individual expects or wants rather than to presume standard expectations. Similarly, education and awareness raising should not be didactic. Education is not an exercise in enlightening the ignorant.

37. Systems have also traditionally been built from the perspective of users behaving rationally and only in ways the organisation expects or desires, e.g. in line with a user manual if there is one. Increasingly, as digital systems become more commonplace, people expect to be able to use any system in any way they might think reasonable. The "affordance" of a system is its ability to be used in a variety of different ways, not just as originally intended. Organisations need to consider how their systems might be used, by both their staff and by customers/citizens, and design safeguards appropriately.

38. Profiling and social sorting is not a science. It needs to be treated with great care, especially if it is being used within a system to limit or restrict a person's entitlements or rights.

Consent for Data Sharing

39. Before building systems that will share personal information, organisation's should consider:
    - Do they have the authority (legal and/or the subject's consent) to share personal information
    - Would they be breaching any applicable regulations
    - Is there a duty of confidence that constrains sharing (though, again, this is not absolute)
    - Applicable advice and guidance, e.g. from the ICO

40. Having the data subject's consent should not be seen as a silver bullet, obtained once to allow any and all subsequent data sharing and use. Information use still has to be fair and appropriate. People will usually understand the need for data sharing but, even so, they will still expect the use of their information to be fair and no more than is appropriate to the consented purpose. And consent applies only to the context and purpose for which it was granted. Presuming consent can be extended to cover a similar purpose under a different context is not safe and should be avoided.

41. Government departments do not always need to obtain the individual's consent. For example:
    - If there is a legal obligation to share
    - If there is a contractual obligation to share
    - If it is not appropriate to ask for consent (e.g. to assist taxation)
    - For covert surveillance