Key Messages from IAAC's People-Centric Information Assurance Workshops 2008-09

Introduction

People are the subjects at the centre of the digital society and the principal recipients of its benefits. They are also the principal bearers of its risks. The central aim of People-Centric IA is to make the systems and structures of the digital society reliable, safe and secure focussing on the interests, concerns and needs of people.

IAAC held three workshops from late 2008 to summer 2009 to develop an understanding of the UK's PCIA needs. The results from each workshop are covered in separate workshop reports. This report summarises the key messages which have emerged from the three workshops together. As with the individual workshop reports, this report is not intended to serve as a record of the workshop discussions. It is, rather, a digest of the many insightful points made during the discussions. IAAC would like to thank the many people who have contributed to its PCIA work over the past year and who have thereby made this report possible.

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

Key Messages

The Direction of Travel

1. To a significant degree, the fabric of people's lives, including the systems and structures with which people engage as they conduct their lives, has been changing. With this change, we have witnessed a huge expansion in the uses being made of personal information.
2. Looking ahead, we might well anticipate a "Moore's Law of personal information". In a few years time, there will almost certainly be much more personal information relating to each of us available over the Internet than there is today. Not only do we each have less privacy today than we have enjoyed in the past but also it is likely we will have less privacy in the future than we believe we still enjoy today.

People Have Concerns

3. In general, people do not object to providing personal information where that information is relevant to a purpose they consent to. However, there are limits to what people are prepared to accept. They start to object when being asked to provide excessive (i.e. irrelevant or unnecessary) information for a consented purpose, and they object strongly to a data gatherer allowing the data that was provided for one purpose to be used for other purposes to which they might not, or have not, consented.
4. People realise that emerging digital capabilities can be very powerful. People's concerns relate not so much to the existence of such digital capabilities but to the ways in which those capabilities can sometimes be used. Some uses can be very positive, but, equally, those same digital capabilities can be used in ways that people could find quite harmful.
5. 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.

A Lack of Sufficient Protection

6. In general, the informational harms people are concerned about can be thought of as the loss of some aspect of their personal capital or well being. They can include harms such as:
    - Serious inconvenience or restriction on one's autonomy;

- Financial loss;
- Reputational damage;
- Emotional stress.

7. Some people are very concerned about these harms, and indications suggest that there is still a significant proportion of people who remain fearful of venturing far on-line for that reason. This limits the extent to which the benefits of the digital society can be realised. The lack of sufficient protection means some people are at risk of exclusion and, overall, the digital society will be slower to develop.

The Role of Privacy

8. Privacy is a long-standing right and has been the cornerstone of how people have protected themselves in the past from information-related 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 weakened as personal information systems encroach more and more into people's lives.

9. For some, privacy is more important than for others. Some people have a strong attachment to privacy and value the protection it provides highly, whereas others, typically youngsters, appear to have less of an attachment to it. As a result, different people view the prospect of the continued erosion of privacy differently. For some, it is a great concern, for others less.

10. However, in either case, if the current level of protection is generally felt not to be sufficient, and if this works as a brake on the development of the digital society, then reduced levels of privacy will only amplify the problem, not address it.

Accommodating Risk

11. That there is always some level of risk in life is unavoidable. However, not everything to do with risk is bad. Risk contributes to learning and to progress. If children aren't allowed to fall over and graze their knees, they miss out on learning how to make basic personal safety decisions for themselves. Similarly, people will learn from the digital risk they experience how to be careful with their personal information. There are benefits to living with risk and we should not aim to eliminate digital risk entirely. To do so would be to stand in the way of progress.

12. Learning to come to terms with and adjust to the increasing presence of digital risk and the erosion of privacy is a challenge all people face, not just the youngest or those most eager to share personal information. Every person today, whatever their chronological age, is part of the first generation of the digital society. We each, in our own way and at our own pace, need to adjust our attitudes and behaviours to the changing landscapes of the digital society.

13. People's attitudes to particular risks can change, as they have done many times in the past and as they no doubt will to particular digital risks in the future. Looking at previous examples of wholesale changes in social culture and lifestyle, people's attitudes to particular risks change as new means to mitigate those risks are developed. Mitigation can include methods of risk sharing, not just of risk reduction. Risk mitigation methods together reduce the remaining risk that has to be accepted by individual victims. This allows people to acclimatise to new sources of risk and for their attitudes to new dangers to soften.

How Things Stand Today

14. Within the UK currently, the level of understanding of, and response to, personal digital risk issues is still relatively immature. In such situations, it is not unusual to find an imbalance in risk practices, with high levels of risk acceptance and low levels of risk mitigation being practiced. This would appear to be a fair characterisation of where we stand with respect to digital risks today.

15. It is often said that the marketplace has a tendency to ignore risk, i.e. that it encourages risk acceptance over risk mitigation, and that therefore we should not expect the marketplace alone to address the present

imbalance. Indeed, some people would say that the level of privacy provided by the market is unlikely ever to be higher than the lowest level of privacy that keeps a digital society sustainable. Possibly we are near to that stage already. It is hard to imagine a more simplistic and unsophisticated approach to privacy than the all-or-nothing 'tick-box' mentality we see so often today.

A PCIA Goal

16. However, this desultory view of the marketplace might not do it adequate justice. The marketplace is multi-faceted rather than simply one-dimensional. It has shown that it is capable, given time, of providing meaningful solutions to present dangers and not only of ignoring risks. As a result, maybe it would be fair to hope that the natural forces in operation within a market-oriented society could lead, over time, to the marketplace providing the types and levels of personal protections people would like to see and which would lead to the greater development of the digital society.

17. This leads us to suggest a goal for the UK's PCIA efforts. By applying appropriate PCIA wisdom to facilitate and accelerate the natural forces in operation, the UK should strive to increase the amount of risk mitigation practised and to reduce the amount of risk acceptance necessitated within the evolving digital society, bringing mitigation and acceptance into better balance, but making sure to do so without resorting to means that get in the way of progress. "In better balance" means raising the level of risk mitigation practised by ordinary people up to a level where the amount of risk remaining to be accepted personally by individuals is no longer a brake on development.

The Path of Progress

18. Though we might look to natural or market forces to do the bulk of the work, we should still try to understand the path or paths the digital society's development might take so we can identify ways to encourage, facilitate and contribute to desired progress. One way to look at progress is to think of it in terms of two orthogonal dimensions, Systems Learning and People Learning. These two go hand in hand and progress requires that advancement be made in both. Hence, the UK should focus its efforts on achieving progress in both directions, not putting all the effort into supporting one at the expense of the other.

Systems Learning

19. 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.

20. 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.

21. 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.

22. 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.

People Learning

23. It is hard to imagine a digital society in which people are not expected to take some responsibility, perhaps the lion's share of responsibility, for their own digital safety and for keeping themselves and their personal information safe. Hence there is a clear need for a comprehensive programme, developing a wide range of materials to alert people to relevant issues, to educate people, and to provide the many layers and levels of advice and guidance people will need.

24. One long-term aim for PCIA should be for children to learn about digital safety in much the same way and at much the same time as they learn about physical safety (i.e. through play, throughout formal education, in the home). However, in the short term, there is a gap to be filled. Today's adults need to learn about specific digital risks and how to stay safe digitally but have not had the opportunity to acquire that learning naturally during their formative years. There is a need for a programme of steps specifically aimed at addressing this short term gap and providing remedial education, formally and informally, to the present first generation of digital citizens.

The Role of Government

25. There is a role for Government in facilitating PCIA progress though it should remain a light-touch role. The Government is, clearly, a stakeholder in the UK digital society, having an interest in the development of a safe and secure digital society. It should decide where and at what level within its operational structure ownership of those interests best lies. It should develop a National PCIA Strategy starting from a vision of what it wants the UK digital society to become over the next five years. It should articulate what it believes its PCIA role and responsibilities to be, and should set out a structured approach to fulfilling those responsibilities.

26. However, Government cannot achieve the UK's PCIA goals alone. There are other actors in the PCIA space, each of which are stakeholders in their own way, and each has a role to play. In particular, there is the need for an agent that can act on behalf of individuals, speaking for their interests and ensuring provision is made for their needs. The ICO would appear to be well suited to take on this role.