Results from the People-Centric Information Assurance Workshop of 12 May 2009

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 giving priority to the interests, concerns and needs of people.

IAAC has conducted two workshops aiming to build a broad understanding of PCIA issues and in principle how those issues might be addressed. The main objective of the first workshop was to explore the nature of how people might use the systems and infrastructures of the digital society, the personal information people might provide gather and use, and the harms people might be caused. The main objective of this, the second workshop, was to look at what might be done in response to the issues raised.

This report is not intended to serve as a record of the workshop discussion. It is, as with the first workshop's report, a digest of many of the insightful points made during the discussion. As with any exploration of a new subject, there are many interlocking ideas to be clarified, organised and understood. The presentational structure adopted for this report is similar but not identical to that used in the first report. As was suggested then, the presentation structure is likely to evolve as the ideas are developed further.

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. We can anticipate a "Moore's Law of personal information" and that, in a few years time, there will be many times as much personal information relating to each of us available over the Internet than is the case today. Not only do we each have less privacy today than we have enjoyed in the past but also we will each have less privacy in the future than we believe we still enjoy today.
2. Different generations weigh the benefits of privacy differently. Older people, typically, have a strong attachment to privacy whereas youngsters appear to have less. If older people are to feel comfortable in the digital society, they will need to acclimatise themselves to their reduced level of privacy.
3. Digital capabilities can be very powerful. The risk issues 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, the same capabilities can be used in ways that the person targeted could find very threatening.
4. Indications suggest that there is still a significant proportion of people who remain fearful of venturing far on-line. However, people's attitudes to particular risks can change. Change has been facilitated in the past when means (technological or otherwise) of risk mitigation and risk sharing have been developed that have had the effect of reducing the amount of a risk remaining to be accepted by the individual victim concerned. This has allowed people to acclimatise to these risks and their attitudes to soften.
5. 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 typical to find overly high levels of risk acceptance and insufficient levels of risk mitigation. This would appear to be a fair characterisation of the current state of concern.

6. A goal is proposed for the UK's PCIA efforts. It is to increase the amount of risk mitigation practised and to reduce the amount of risk acceptance necessitated, bringing the two into better balance, without resorting to means that get in the way of progress. "In better balance" means the level of risk mitigation practised is sufficient that the remaining risk can be accepted through a combination of risk sharing and personal risk acceptance by the victim.

7. Our analysis of how societies have responded in the past to the emergence of new social risks suggests that the natural forces in operation within a free, market-oriented society, perhaps facilitated and accelerated by appropriate PCIA wisdom where appropriate, can reasonably be expected to achieve this goal.

8. Even though we might look to natural forces to achieve that goal, we should still try to develop an understanding of the path or paths that we expect will be taken, this so we can identify ways to encourage, facilitate and contribute to progress. The path of progress as it is made can be understood in terms of two orthogonal dimensions, Systems Learning and People Learning. There are limits to what can be achieved by progress in each direction, so encouragement, facilitation and positive contributions are needed in both directions, not just in one direction or the other.

9. 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 the operational structure of Government ownership of those interests best lies. It should develop a National PCIA Strategy starting from a vision of what it wants the UK to achieve in the next five years. It should articulate what it believes its PCIA role and responsibilities to be, and set out a structured approach to fulfilling those responsibilities.

10. 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.

11. 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. However, this means that in the short term, there is a lacuna to be addressed. 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 during their formative years alongside learning about physical risks. There is a need for a programme of steps specifically aimed at addressing this transient hole and providing remedial education, formally and informally, to the present first generation of digital citizens.

The World and the Way People Live is Changing

1. Information flows between data subjects and data holders are normally heavily asymmetric. Providing people with the ability to make subject access requests starts to redress that asymmetry, and as a result can help to rebalance the relationship between people and their service providers.
2. Nowadays, we each have the ability to stalk each other, whether through social network sites, people search engines or other means. Using tools such as these to find out a little information about someone else, either for general interest or in preparation for an introduction, would be considered by most searching parties to be perfectly acceptable. People should assume 3rd parties search for information about them as much as they as 3rd parties might do so about others.
3. We can anticipate a "Moore's Law of personal information" and that, in a few years time, there will be many times as much personal information relating to each of us available over the Internet than is the case today.
4. It is clear not only that we have less privacy today than we have enjoyed in the recent past but also that, unless society works to counter the trend, we will each have even less privacy in the future than we believe we still enjoy today.
5. This erosion of privacy means that people are being made increasingly vulnerable to what 3rd parties might choose to do with their personal data, and are becoming increasingly exposed to the unwanted outcomes that arise from the things those 3rd parties do.

People's Attitudes and Expectations are in Flux Too

6. Different generations weigh the benefits of privacy differently. Older people, typically, have developed a strong attachment to privacy. Privacy serves as a control people use to limit what others can do with their personal information. Any erosion of that privacy they feel as an increase in their vulnerability and hence as a source of anxiety. Youngsters do not appear to have such a strong attachment to privacy. They also tend to have a stronger interest in building social capital, the social credit of visibly having lots of connections and being in the middle of a large group of friends. They do not feel their current level of reduced privacy as a heightened level of vulnerability and hence do not see this as a source of much anxiety for them.
7. If older people are to feel comfortable in the digital society, they will need to acclimatise themselves to their reduced level of privacy and learn that they do not need to feel so anxious about their vulnerability.

Any Change Brings Risk. The Harms People Might Suffer.

8. The first impression a person makes on the Internet in some ways carries more weight than the first impression a person makes in a closed social group. A wider group of people can be exposed to that first Internet impression and it can persist in corners of the Internet even after it has been countered elsewhere by other more balanced impressions.
9. The effectiveness of Chatham House rules requires the co-operation of every person in the room. Today's consumer electronics allow anyone in the room to record a discussion stealthily. Weakening respect for privacy rules make it increasingly likely that a 3rd party will then make details from their recording, if not the recording itself, public. People cannot rely on co-operative privacy rules for their protection as much as they might have done in the past.

10. The number of links a person has on social networking sites and the types of links they have can tell an enormous amount about that person, including things (e.g. sexual orientation) that they might not be happy to volunteer.

11. A person cannot opt out of the information society. There is an enormous amount of information about each person publicly available on the Internet, even if the person considers themselves to be a non-adopter of digital technologies. All people are exposed to digital society threats even if they do not participate in the benefits.

12. Digital capabilities can be very powerful. These capabilities are a mixed blessing. The risk issues relate not so much to the existence of these new capabilities but to the ways in which those capabilities can sometimes be used. Some uses can be very positive. (One example mentioned was of a person who was able to find his long-estranged sister only due to the power of new digital channels.) But, equally, we can all imagine how the same capabilities could be use in ways that the person targeted could find very threatening.

13. For example, one new powerful digital capability has led to the emergence of 'people search engines' through which a 3rd party can find all sorts of information about almost any person. Most of the time, the information discoverable this way is non-sensitive information that is already easily found in the public domain. So long as the power of these people search engines is limited to searching easily available public information, they are unlikely to represent much of a risk to most people. However, the perception of the risk could change as soon as people search engines become significantly more powerful. The risk would probably be considered to be much higher if, say, Google were to provide a people search service.

14. The ability to find data without needing to know beforehand where it is located and then to bring dispersed data together is a game changer. It might be that no one site holds enough personal information to represent much of a risk to the data subject but when dispersed information is brought together the aggregate can be sufficient to enable the subject to be caused significant harm.

15. eCrime is expected to grow as the roll-out of broadband to people's homes advances. Just as the growth in spam and malware have tracked domestic broadband growth, so too will eCrime.

People's understanding and attitudes to risk.

16. Indications suggest that there is a strong appetite amongst people to shop on-line but also a significant proportion of people who remain fearful of venturing far on-line. For them, the general risk, as they perceive it, is still sufficiently high that they are not willing to accept it.

17. People's attitudes to particular risks can change. One possibility is that people might come to realise that the likelihood of a particular outcome is much less than they had originally feared. Alternatively, people's attitudes to a particular unwanted outcome can change. One example of this is credit card fraud. Credit card fraud is nowadays seen increasingly as a significant inconvenience rather than as a major horror, a bearable contemporary hazard rather than a personal disaster as before. This particular attitude change has been facilitated by having card issuers pick up the fraud losses rather than have the losses be borne in full by the individual victim. The card issuers then recover those losses through their service charges. In this way, each person's fraud loss is dispersed and shared out amongst the whole community of credit card users. In this way, financial institutions provide credit card users with a safety net that protects them from harm when they get hit. With the harm reduced, people are more likely to perceive the risk of credit card fraud as bearable.

18. However, such softening of attitudes to a risk does remain conditional upon the risk's frequency. Risks can be perceived as acceptable provided they do not happen too often. Being the victim of credit card fraud once every several years might be considered unwelcome but bearable. Being a

victim several times a year probably would be seen as something much more serious and altogether not acceptable.

19. There are some risks where the undesirable activity does not remain infrequent. Some undesirable activities, when first emerging, take place only on a micro scale. Then, at some stage, the dynamic changes and the activity becomes macro scaled. An example of this is spam. Spam levels have gone from one in many thousand e-mails when spam was new to about 70% of all e-mails today.

20. In cases such as this, risk mitigation measures rather than risk sharing measures are needed to make the risk bearable. E-mail is still used heavily by people despite the enormous levels of spam present. Technologies have been developed to enable people to cope more easily with spam, e.g. anti-spam filters that can differentiate sufficiently between legitimate e-mail and spam. In this way, technology has kept people's risk small by containing the otherwise rampant growth of a very low impact event. Hence, attitudes to spam have acclimatised to accommodate spam even though the level of spam has grown enormously.

21. Social networking has enjoyed enormous growth in the past five years. Currently, it is believed that only a tiny fraction of social network profiles are fraudulent. There is clearly the potential for that fraud rate to grow. If a dynamic were to change causing the fraud rate to grow to a much greater level, past experience suggest we can expect that a number of things might happen in response. Possibly, means will be developed (technological, such as profile scanners, or social, such as the eBay feedback process) to distinguish reliably between true and fraudulent profiles. Otherwise, perhaps the way profiles are created and constructed will change to maintain profiles' general reliability. Or ways will be found to create a safety net (through sharing or otherwise) to alleviate the harm a fraudulent profile causes.

22. Many of the risks people associate with the digital society have not yet moved beyond the micro scale. It can be expected that, with time, some of them will. As each one does cross over to the macro scale, it can be expected that, as in the past, risk mitigation and/or risk sharing solutions will be developed to keep the risks bearable.

Vision

23. For progress to be made addressing personal digital risk issues, it would be helpful to have a vision of what the ultimate end point of the UK's PCIA efforts could be. That would help us to identify one or more goals lying in that direction, and, at the same time, to suggest a plan of attack that could be successful in achieving those goals.

24. What should the vision be for PCIA in the UK? An earlier UK Government vision was to make the UK the best place in Europe to do eBusiness. Maybe the aim of PCIA should be to make the UK the best place in Europe to be an eCitizen, a citizen of a fully fledged, fully functioning, safe and secure national digital society.

Goals

25. The world of personal information is changing radically, not evolutionarily. We are at a 'phase transition', a change in state. In keeping with common experience, we must work with progress rather than try to stand in its way. King Canute symbolises the futility of trying to hold back progress. We need to learn to ride the wave of digital progress, though maybe on surfboards that come with safety helmets and straps for holding on.

26. With that image in mind, what goals might we propose for PCIA? As was discussed in our first workshop, within the UK currently, the level of understanding of, and response to, personal digital risk issues is still relatively immature and simplistic. In such situations, it is typical to find overly high levels of risk acceptance and insufficient levels of risk mitigation being practised. This

suggests that one goal for PCIA could be to increase the amount of risk mitigation practised and to reduce the amount of risk acceptance necessitated, bringing the two into better balance without resorting to means that get in the way of progress.

27. What might 'in better balance' mean in this context? Risk mitigation is a combination of many measures, including capping the likelihood of unwanted harmful outcomes and reducing the impacts associated with such outcomes. Risk acceptance can take the form of either acceptance of the residual harm by the individual concerned or, where all or part of the harm is transferable (or compensatable), sharing acceptance of that transferable part of the residual risk amongst a community at large. As the credit card fraud example has shown, sharing residual risk in this way provides a safety net to reduce the harm caused to the individual victim.

28. Possibly, then, the balance sought in that PCIA goal might be to reach a situation where there is a sufficient amount of risk mitigation practised given the level of threat that two conditions are met:

    - The user community at large is able to accept sharing as a way to cope with the transferable part of theirs and other people's residual risk (i.e. each person's share of other people's risk is sufficiently low once the risk is shared across the community as a whole);

    and

    - The non-shareable part of the risk that remains is sufficiently low it can be accepted by the individual victim (i.e. the remaining impact on the individual is bearable given how frequently or infrequently the problem happens to them).

29. There are a number of ways risk can be shared. As we have seen, credit card fraud provides one example. Another way societies share risk is through insurance. Insurance provides a democratic means by which the market sets explicit standards for personal prudence and shares the transferable or compensatable part of the remaining risk. It also puts prices on the risk differentials between different standards of prudence. Then, if a person can't find an insurer to cover them at what they consider to be an acceptable price, they either increase the amount of risk mitigation they practise themselves or accept a larger proportion of the risk for themselves.

30. Some people will continue to practise risky behaviours regardless of the risk. For this reason, on the risk mitigation side of the balance, there should be a strong focus on how to deal with the consequences of unwanted outcomes not just a focus on how to reduce the likelihood of unwanted outcomes. Societies have followed this approach in the past. The rise of the permissive society led to the increased adoption of ways of coping with the consequences of new permissive behaviours, e.g. pregnancy terminations, not only to increases in methods that reduced the likelihood of such outcomes (such as contraception). Interestingly, it also led to a softening in the general attitude towards the residual risk, i.e. the acceptability of having children born out of wedlock.

31. This analysis suggests that the goal proposed earlier for PCIA is feasible. We should reasonably be able to expect that the natural forces in operation within a free, market-oriented society, perhaps facilitated and accelerated by appropriate PCIA wisdom, are capable of taking the UK forward to a situation where there is an appropriate balance between risk mitigation and risk acceptance without the need for a level of intervention that would count as standing in the way of progress.

Approach

32. Even though we might look to natural forces to steer the UK towards that goal, we should still try to develop an understanding of the path or paths that we expect progress to take. This is so we can identify steps that could encourage, facilitate and contribute to that progress whilst not impeding or crossing the grain of that progress.

33. One suggestion was that we should try to understand the path of progress in terms of two orthogonal dimensions, Systems Learning and People Learning, and that we should aim to foster progress in both. There are limits to the progress that can be achieved in each direction alone, so contributory action in both directions is needed, not a focus on just one direction or the other.

34. Systems Learning and People Learning are not just about building smartly secure digital systems and then teaching people how to use those systems securely. Systems Learning is much broader and is concerned with the organisational systems and structures put in place to facilitate the operation of a safe and secure digital society. It includes:

    - The arrangements created of roles and responsibilities, of ownership and accountability, of powers and checks. These arrangements might include new bodies created specifically to discharge certain responsibilities such as supervision and reporting;
    - The policies, legislation, regulations, oversight and enforcement created to give form and shape (and boundaries and transparency) to promoted behaviours and practices.

35. People Learning is similarly broad. It is concerned not only with teaching people how to use digital systems securely but with all aspects of getting people to settle upon sensible behaviours and practices that enable them to cope with the risks inherent in their behaviours. This includes:

    - Sensitising people so they can acknowledge there are issues affecting their personal safety that demand their attention;
    - Educating people regarding the dynamics that threaten them and the ways they could be harmed;
    - Providing people with advice on the simple things they can do to protect themselves, and how;
    - Helping people to equip themselves with further information and understanding so they can make competent decisions regarding the precautions and risks they might elect to take.

We shall look at both Systems Learning and People Learning in a bit more depth.

Systems Learning

The Role of Government

36. The Government is, clearly, a stakeholder in the UK digital society, having an interest in the UK's digital future being reliable safe and secure for the citizens of the UK. Given that part of the goal for PCIA is to avoid resorting to means that get in the way of progress, the Government's approach to protecting this interest should not be a heavy-handed one.

37. The current Government, and departments such as BERR, have demonstrated a measured approach to introducing regulation and a reluctance to regulate unless regulation is clearly required. This is in line with the above principle. However, some regulatory activity is called for. UK business does need an enabling regulatory framework if it is to contribute to PCIA progress. Otherwise commercial pressures plus the potential legal exposures can limit business' freedom to act constructively. Hence, Government should be prepared to act where its activity can enable and support others. Its approach should be a light-touch one and not a hands-off one.

38. With this perspective in mind, Government should confirm its ownership of the national PCIA interest and, in so doing, acknowledge that it is for the Government to take the lead and that there are some important issues that will need its engagement. It should decide where within the operational structure of Government that ownership should best lie and should ensure that ownership is held at a sufficiently high level given the strategy and agenda that will be forthcoming.

39. As a next step, the Government should develop a national PCIA strategy based on a vision and an approach it believes appropriate. The UK Government currently has a National IA Strategy. However, this strategy has been criticised for not articulating a vision of where the Government wants the UK to be in five years' time, and for not giving adequate consideration to the individual, i.e. for not being adequately people-centric in its approach. Hence, the UK Government should develop a strategy specifically for PCIA that reflects the UK's PCIA interest, issues and needs. This could be positioned under the broader National IA Strategy if required.

40. The Government should then develop a structured approach to executing its strategy and delivering what it believes its responsibilities to be. One structured approach, that was referred to as 'broad regulation', would entail:

    - Defining the scope of the Government's role and its responsibilities. This could cover, for example: policy formulation; the development of enabling legislation and regulation in line with policy; putting that legislation and regulation into effect; enabling the provision of compliant services by public and private sector bodies; oversight and enforcement;
    - Identifying which bodies will take forward which roles and responsibilities within a structure arranged so that policy can be consistently and uniformly promoted throughout and policy interpretation made compliant with policy intent;
    - Ensuring those bodies have the expertise and discretionary powers (delegated authority) required for the fulfilment of those responsibilities. Also, ensuring that their actions can be adequately and publicly scrutinised and the bodies held to account. This would enable the responsive and effective fulfilment of responsibilities at each level.

The Steps Government Can Take

41. Government should set required PCIA practices for the public sector and ensure enforcement has teeth. That would provide a good foundation from which to lead a wider improvement in information safety and security practices across all sectors and participants.

42. Whatever enabling regulation the Government decides upon should be structured in the form of a set of basic PCIA principles rather than a detailed set of rules. A principles-based approach is held to have contributed to the success of the DPA in its early days when the use and management of personal data by organisations was in its infancy. Given that the current understanding of digital risk issues is similarly in its infancy, a principles-based approach would seem appropriate. It would be likely to have greater longevity during a period of extensive change than a purely rules-based approach.

43. With all due regard to the successes the DPA can rightly claim, the Government should not simply adopt the current DPA principles as its starting point for a set of PCIA principles. The DPA was created before the Internet and PCs became widespread. The risks today are different in both nature and magnitude from those present in the early 1980's. For example, technology has freed people and 3rd parties from needing to know anything about where data is held before they can access and use it. There is a case to be made that the DPA's principles should be brought up to date with the modern age.

44. Considerable experience working with data protection principles has been gained since the early 1980's. That might be sufficient to enable the UK to consider supplementing a principles-based PCIA approach with a number of interstitial rules that clarify the application of basic principles in spaces where conflicts might arise. PCIA rules might, for example, cover matters such as: when explicit acknowledgements of data use should be provided to people; the requirements for auditable records; methods to provide transparency; provisions for subject-initiated review of data held; requirements for correcting or countering errors; defining data handler accountabilities; and so forth.

45. Rules embody standards. In the first instance, PCIA rules might simply embody a set of minimum standards participants are generally prepared to accept. As PCIA experience grows, rules can be strengthened if necessary to provide a rising platform raising standards in specific areas of conflict up to a higher level.

46. Thinking further ahead, the UK requires type approval for automobiles, varying according to the type of vehicle. This is so no vehicles are authorised for sale in the UK unless they have acceptable levels of personal safety built in. In due course, the Government might consider introducing a simple form of PCIA type approval for personal data services, varying according to the type of service. Under this approach no system, whether it be a national identity system, public sector entitlement system, private sector personalised service system, social networking site, or content sharing site, would be authorised for use within the UK unless it met the standards set by the Government for reliability, safety and security.

47. To help ensure the success of its PCIA actions, the Government should consider if there are lessons to be learned from the way Health and Safety has achieved its success over the past 20 years. Health and Safety has been successful in that the UK's considerable H&S interests are addressed today by a mature body of regulation and legislation universally applicable within the UK and supported by supervisory agencies receiving in aggregate over £1billion of Government funding. The answers to the question of what contributed to the early stages of H&S's success could provide lessons for ensuring the success today of PCIA.

The Role of Other Stakeholders

48. However much of a role, large or small, the Government takes on, Government cannot achieve the UK's PCIA goals alone. The state can provide leadership and policy and regulation but it should not try to be ubiquitous. There would be no support for a 'nanny state' in this aspect of national life. Other actors, which includes service providers, the public, educators, the media, even informal groups acting on behalf of particular communities (e.g. the technologically disadvantaged, children) are each stakeholders in their own way and each has an important role to play.

49. Data holders hold personal information about people on trust. That implies they have an obligation to keep that information current, accurate and safe. Social network sites are holders of personal data. Even though social network sites do not have a commercial relationship with their users (there is no commercial transaction taking place), they do still have a direct relationship with their users and this relationship imposes trust obligations upon them.

50. Given the continued power asymmetry between service providers and individual users, there is a role to be played by an agent that would 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. The ICO has grown stronger and more active in recent years, its sphere of activity includes education and awareness as well as review and enforcement, and it has attached itself to the PCIA issue.

People Learning

51. It was suggested that there are four pillars to effective People Learning: Alert; Educate; Advise; Guide.

Alert

52. An essential first step is to alert people to the issue of personal digital safety. People won't pay attention to education and advice, and, more importantly, won't change their behaviours and practices, until they have understood that there is an issue before them that needs their attention.

53. If there are matters that people need to know about, e.g. the threats and risks they face, people should be told about these in a direct and unadorned manner. People are more likely to be moved to action if the threats are presented to them plainly than if the issue is presented in a gentler, less direct manner. People respond more when pushed than pulled.

Educate and Advise

54. Once people have been alerted to an issue, their immediate requirement is to be helped to address that issue. The objective is then to communicate relevant risk-related information to people without scaring them off. Scaring them off can be avoided by offering them plain-language advice on a small number of simple steps that they can take immediately to address the core of the newly presented issue. Hence, education and advice go hand in hand as one.

55. People learn about physical risks and about how to stay safe physically over many years as they grow up and from a variety of sources: in school; in the home; in the activities they participate in. Additionally, the lessons they learn are primarily about specific physical risks and specific methods for dealing with those risks (how to cross the road safely, how to handle matches, to stay away from strong river or sea currents, etc.).

56. 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. Education in school implies introducing digital safety education and advice into formal state-sponsored education. Education at home implies having parents who are already digital-safety aware. Hence, there is a need for adult education courses that equip parents to educate their children. Education within the activities youngsters participate in implies a loosely structured approach involving a wide variety of tricks and tools being pushed out via the Internet and the web.

57. As has been the case for physical safety education, the content of digital safety education should be specific. It should cover teaching people about specific risks, how to avoid those risks, and what to do if they should be unfortunate enough, or careless enough, ever to have an accident.

58. In the short term, there is a lacuna to be addressed. Today's adults need to know about digital risks and how to stay safe digitally but have not had the opportunity to acquire that knowledge during their formative years. In addition, today's youngsters can be closed to learning essential digital safety messages from their elders as many of their elders have little 'street credibility' in a youngster's digital world. Hence, 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.

Guidance

59. The fourth pillar to effective People Learning is guidance, helping people to equip themselves with further information and understanding so they can make competent decisions regarding the precautions and risks they might elect to take. For example, it is important to tell people when it is their personal responsibility to take precautions or to behave carefully, as otherwise they will tend to assume someone else is taking care of the issues for them.

60. Guidance also includes steering people to where they can get authoritative information about particular issues they might be concerned about, presented in a way that is designed to be accessible to them. This implies, of course, agreement on what constitutes authoritative guidance and good advice.

Tailoring the Delivery

61. Though the general purpose and content of digital safety messages will be broadly the same for all types of people, effective delivery means the form and style in which safety messages are communicated should be tailored to the audience.

62. The audience for safety messages should be segregated (perhaps by age, gender, into characteristic groups) and an appropriate medium and style for conveying the messages to that group selected. Traditional 'public service message' forms of communication are unlikely to work with a group used to taking in information presented in a more light-hearted and visually imaginative manner.

63. The private sector can be of assistance here. Retail marketeers have developed a considerable experience and expertise in conveying brief specific messages to each type of audience. They are familiar with the art of segregating the audience according to the nature of the content being conveyed, and with developing imaginative ways to turn domain-specific knowledge into messages people can understand.