Results from the People-Centric Information Assurance Workshop of 5 November 2008

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.

The primary objective of this, the first in a series of workshops, 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. A secondary objective was to begin to consider how some of the issues raised might be addressed.

This report is not intended to serve as a record of the workshop discussion. It is, rather, a digest of many of the insightful points made during the discussion, organised according to a structure that has suggested itself only during the preparation of this paper. As with any exploration of a new subject, there are many interlocking ideas to be clarified, organised and understood. To provide some initial structure to this report, the ideas have been organised according to whether they illuminate the problem space or the solution space. This structure may be superseded by a more meaningful structure as ideas are developed further.

The subject matter organisation used here is, then:

- The Problem Space
    - The world and the way people live is changing.
    - People's attitudes and expectations are in flux too.
    - Any change brings risk. The harms people might suffer.
    - People's understanding and attitudes to risk.
- The Solution Space
    - Setting out – Vision and Perspective
    - Setting out – Approach and Principles
    - Making Progress – Governance
    - Making Progress – Controls and Techniques

Throughout this paper we shall conform to the following terminological distinction.

- "People" means private individuals using the systems and structures of the digital society as they go about their normal lives. Generally, they are the subjects to whom personal data relates.
- "3rd parties" are the other entities with which people engage in the process. These are, in a general sense, the users of people's personal data. Many of these will be people themselves (e.g. Facebook friends, malicious individuals), or people acting on behalf of a non-personal body such as a corporate entity of government department.

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. In a not insignificant way, the fabric of people's lives, including the systems and structures with which they engage as they conduct those lives, is changing. With this change, there has been a huge expansion in the uses made of personal information.
2. In general, people do not object to providing personal information explicitly where that information is relevant to a purpose they consent to. However, there are boundaries to what people are prepared to accept. They start to object when 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.
3. Privacy is the primary means people have to protect themselves from information-related harms to their interests. Hence, privacy serves as a control. What this means is that privacy invasion should not be thought of as a harm in itself. It is, rather, a weakening of one of the central protections people use to help prevent actual harms being caused.
4. Harms can be considered the loss of some aspect of personal capital or well being. From this perspective, harms would include damage such as:
    - Serious inconvenience or restriction on one's autonomy;.
    - Financial loss;
    - Reputational damage;
    - Emotional stress.
5. There remains a lot of work still to be done to understand better the harms people can suffer in the digital world.
6. Just because people sometimes act unsafely doesn't mean they don't realise there are risks or that they don't care. Many people find risk a difficult concept to work with. They find it hard to believe in the reality of risks until they see them materialise in a way that affects them or people close to them. As a result, people often do not make personal risk decisions well.
7. Some risk is unavoidable, otherwise there would be no learning or progress in the digital world. 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 experience how to look after their personal information. We should acknowledge these learning processes and we must ensure that whatever we do we do not stand in the way of progress.
8. It is normal practice to presume that the marketplace alone will not cater for all the risks. The market has a tendency to ignores risk, meaning that it encourages risk acceptance at the expense of risk mitigation. As a result, the level of privacy provided will fall to the lowest level sustainable. Possibly we are there already. It is hard to imagine a more simplistic unsophisticated approach to privacy than the all-or-nothing 'tick-box' mentality we see so often today.
9. However, maybe this view of the marketplace does not do it justice. The marketplace is multi-faceted rather than simply one-dimensional and it is capable of doing more than just ignore risk. Perhaps in time it will provide the personal protection we would like to expect.
10. It is hard to imagine a digital society in which people are not expected to take some responsibility, if not the lion's share of responsibility, for their own digital safety. Responsibility for safety will necessarily be distributed with different parties having a different share of the pie, and people as individuals will be expected to take their share of responsibility for keeping themselves and their personal information safe.

11. Educating the user doesn't, on its own, address the whole problem, but it does help and should be considered one part of the solution even if it is not the whole solution. However, educating the youthful user is a difficult challenge. The adults best placed to have influence over the behaviour of digitally active youngsters are those within the milieu, i.e. the owners of the components (Microsoft, Google, Facebook, EA Games). These organisations have to be engaged in the process of providing appropriate education to people.

The World and the Way People Live is Changing

1. ICT and digital information are becoming increasingly central to service provision as the UK becomes increasingly a digital society. And for the services people take or the facilities they use on-line, often that digital information takes the form of personal data.
2. This creates a pressure on people to provide personal data to a wider range of 3rd parties and to allow broader use of their personal data. Government claims services could be more joined up, convenient and personalised if only people would allow data already provided to be shared between departments. Protection services claim they would be able to protect people more effectively if only people would give those services more visibility over them and if they identified themselves more frequently.
3. It is not only in the 'business' side of life, where people take services or receive benefits or engage asymmetrically with corporate or government entities, in which there is this trend towards the greater use of personal information. In the social side of life too there is a trend for the wider sharing of personal information.
4. People have a desire to say who they are, for self-definition. It used to be that our class, our clothing, our mannerisms and our jobs said who we were. These channels for self definition are waning, due in part to lower barriers to class and cultural mobility, wider tertiary education and to careers being less unchanging. This helps to explain the popularity of social networking and user-created content sites; they serve as replacement channels for self-definition.
5. The social aspects of social networking provide people with a way to declare and demonstrate who they are. The networking aspects of social networking mean that, in so doing, people make themselves and their relationships more visible.
6. As a result, people live a more widely visible, accessible and non-anonymous life these days. People voluntarily make themselves more visible through social networking sites. People are also made more visible through state and civic surveillance. The mobile phone and IM have made people increasingly accessible to their friends. People are also increasingly accessible to unsolicited 3rd parties who might want to sell them something or exploit them. People are less anonymous, often having to identify themselves when accessing an on-line service even if that is only so the service provider can address them personally. Increasingly, people also have their anonymity eroded through the growing variety of ways in which they can be recognised or identified at a distance without their needing to consent to identification or without their explicit provision of identifying information.
7. A discussion of these changes today might focus on on-line services and on-line shopping and on the social interaction media currently in widespread use: mobile phones; IM; Skype; social networking sites; Twitter; multiplayer on-line games; Google Street View; and so forth. Some of these media are likely to be transient, and new media and applications will rise to prominence in the coming years. Whatever understanding we form or course of action we decide to venture upon, we need to recognise the speed of these changes and not lock our thinking or solutions to today's digital landscape.

People's Attitudes and Expectations are in Flux too

8. For a long time (but only since industrialisation - it has not always been so), privacy has played an important role in people's behaviours and in the behavioural expectations they have of others.

9. Privacy is about controlling the uses made of one's personal information. It provides people with a way to cap their vulnerability to the unwanted actions or attentions of other people. Privacy is about restricting who has access to one's personal information only in so far as restricting access serves to control the uses a 3rd party might make of one's data.

10. Surveys indicate that people are still interested in privacy, even though we might sometimes think otherwise. People often have a confused or unclear understanding of the purpose of privacy or how it is achieved. This might explain why people do not always act in a way that preserves their privacy, leading to the perception that they no longer care for it. People sometimes miss opportunities to protect their privacy, and once the opportunity has passed it can be difficult to retrace one's steps or return to the *status quo ante*. However, there are also many situations where people do demonstrate their desire for privacy and act to protect it. For example, children modify their behaviours in response to the risks they perceive, such as protecting themselves from the risk of mum or dad seeing what they are doing on-line.

11. In general, people do not object to providing personal information explicitly where that information is relevant to a purpose they consent to. They start to object when 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.

12. Sometimes data gathering is covert, possibly as a way for data gatherers to circumvent the reticence, concerns or objections people might have. For example, gathering personal data from children in the guise of them keeping their personal pet alive, or the applications on social networking sites that gather data under the pretext of a competition or quiz.

13. Sometimes data gathering is implicit rather than covert, such as with the use of CCTV or customer loyalty cards. And the greater the transparency of that implicit data gathering, the greater the consent that may be implied. The surveillance aspects of the digital society are not something wholly imposed upon us.

14. People provide implicit consent knowingly to CCTV, as in this case monitoring and the recognition of people is the primary purpose of the system. People provide implicit consent less knowingly when they use their loyalty and payment cards, as in these cases profiling is only a secondary purpose and monitoring perhaps a tertiary one. People provide implicit consent unwittingly or perhaps not at all when they use open communications systems such as telephones, e-mail and the Internet, as in these cases gathering data for the purposes of monitoring or identification could be considered an abuse of privilege.

15. There are boundaries to what people are prepared to accept. There is a point at which surveillance starts to become intrusive. There is a point at which greater accessibility becomes an annoyance. There is a point at which the citizen's willingness to waive their privacy for societal benefit (e.g. for better protection against crime or terrorism) ceases and their refusal to co-operate with the operations of the state starts.

16. Behaviours are to a degree context specific (someone might behave differently in front of their in-laws than in front of their drinking buddies). Therefore it is the arrival of new contexts and new situations that provide opportunities for behavioural churn and evolution. As the digital world continues to introduce new contexts and situations, we should expect behaviours and attitudes to continue to change.

17. People can maintain different behaviours in different situations only to the degree that they are able to maintain separation between their social domains. To the degree that the social use of

ICT weakens compartmental boundaries, behavioural contentions arise. People then have to decide which behaviours to change in which situations. In this way, new behaviours can replace existing behaviours in familiar established contexts and situations.

18. Hence, we should remain open to the possibility that the role of privacy tomorrow might be a little different from the role it has today. Also, that the role it has acquired for some people today might already be a little different from the role it has traditionally been thought to play in the past.

The Harms People Might Suffer

As well as providing many new benefits, change brings new opportunities for people to be harmed.

Many of the ways in which people can be harmed in the digital world will be familiar from the physical world. They are the digital analogues to the harms people can suffer in the physical world. Others will be new or in some way substantially different from their closest physical analogues. Harms can also arise from the inappropriateness of applying physical world expectations to the digital world.

19. Digital world data does have different attributes to physical world data with respect to its retention, accessibility, discovery, aggregation, mining, recoverability, and so forth. This applies as much to personal digital data as it does to non-personal digital data. With the proliferation in the use of personal digital data, the threats relating to the use of personal information, the range of possible or likely outcomes from the use of that information, and the harms that people can suffer, in the digital world can all be different in both nature and number from their analogues in the physical world.

20. What are the harms that people can suffer in the digital world? The central harms are the harms to a person's best interests that can arise from the use of their personal information by a 3rd party. People have a huge range of interests they would like to protect, and personal information can be used in a huge variety of ways that can be contrary to those interests.

21. Privacy, as a way to control what 3rd parties might do with a person's personal information, is the primary means people have to protect themselves from information-related harms to their interests. Hence, privacy serves as a control. Privacy invasion is not, then, a harm in itself, it is a weakening of one of the central protections people use to help prevent actual harms being caused. Privacy invasion can enable someone to locate a person they might wish to harm or to identify a vulnerability through which they can cause a person harm. But privacy invasion is not a harm in and of itself.

22. Harms can be considered the loss of some aspect of personal capital or well being. If so, what then are the harms people can suffer?

23. Serious inconvenience or restriction on one's autonomy is one harm.

    - Data acquirers can do anything with data (subject to compliance requirements, which are often weakly enforced and then mostly in retrospect after there has been a failure). This includes losing it or not keeping it accurate. As a result, someone might be declined a service or access to an entitlement, or might find a desired service or facility is not available to them when they want or need it. This has long been the case in the physical world. As people grow to rely increasingly on personal digital information as the feedstock of service delivery, they feel this exposure more frequently.
    - Profiling can be performed more easily now than in the past. But profiling is not a science and can lead to either incorrect judgments being made or unintended consequences arising. Hence, profiling is a growing avenue that can lead to people being treated unfairly and thereby caused serious inconvenience (or other forms of harm).

- Behaviours are context-specific and people may well wish to project different personae in different situations. One's public face can be different from one's private face. However, with the greater accessibility and discoverability of digital data compared to physical world data, what a person presents to one community of people on-line can more easily become known to others elsewhere. What people say in one place (e.g. a social networking site) can contribute to the basis on which 3rd parties make judgments that affect their interests in other situations or contexts (e.g. university applications). People feel this as a restriction on their freedom to manage their relationships according to the specific contexts and interests of the individuals involved. Celebrities suffer this restriction already.

24. Financial loss is a second harm.
    - Identity theft is one well known way in which people can be caused serious financial harm. This is perhaps the one that most people, if asked, would mention first.
    - There are other ways short of full identity theft by which people can be caused financial loss. For some time, user authentication for personal on-line financial services has relied on the user's knowledge of private but not secret personal information. Increased disclosure of personal data can facilitate specific financial loss such as the unauthorised use of a single bank account – harmful whilst remaining short of full identity theft.
    - HMRC lost 25 million personal data records covering over seven million families. (Try losing 25 million paper records!) It is not known that any person has suffered financial or other harm as a direct result of this loss. However, the threat to them remains and people's vulnerability has increased, even in the absence of recorded harm.
25. Reputational damage is another harm. A person's reputation has value. It is part of a person's personal capital and something they use to sustain their wellbeing.
    - Reputation is how people are perceived by others. A person's reputation affects how 3rd parties make judgements and decisions that have a bearing on them. Hence, reputational damage can affect the relationships a person has with others in a wide variety of ways, and this can lead to unfair treatment, disadvantage, serious inconvenience, financial impairment.
    - As an aside, another aspect of HMRC's and MoD's loss of personal data has been the reduction of public confidence. This could hurt these departments' abilities to prosecute their missions (e.g. HMRC's ability to collect revenue in the future, or the MoD's ability to recruit into the armed forces). To the degree that reputational damage has been suffered by the Government generally, all parts of Government could find their ability to prosecute their missions impaired.
26. Emotional stress is another harm.
    - People can enjoy enhanced autonomy and freedom to express themselves on-line as being on-line can reduce their risk of being recognised. "On the Internet, nobody knows you are a dog!" This might be seen as one of the benefits of digitisation. However, one person's greater freedom to express themselves is another person's licence to misbehave. Hence, people can be upset, offended or bullied – caused emotional harm by the behavioural licence taken by 3rd parties. In extremis, they could become seriously fearful for their wellbeing due to the behaviour of a malicious 3rd party.
    - Being treated unfairly (which is an outcome made possible in many ways by the incorrect or inappropriate use of personal information) can lead to people feeling frustrated and angry, especially when the act is committed by their government, as then people might feel they have little ability to reverse the result or prevent a recurrence.

27. Sometimes the harm can be unintentional. For example, the societally beneficial use of ANPR data can lead to a loss of individual privacy and various consequential harms. That the primary purpose of a proposed gathering of data might be a benefit for society is not sufficient to ensure that that gathering of data will not be harmful.

28. As well as considering the harms people can be caused through the use of their personal information, we should consider the ways in which people can find themselves more vulnerable on-line than in the physical world. For example, through ICT connections people engage with other people without their usual ability to form impressions or judgements relating to those people based on what the person looks like, their body language, etc. Hence, people have to base trust decisions on the remaining behaviours they are able to see as mediated by the digital channel being used (which we can expect will increasingly include a visual component, such as in the use of live video with Skype). Where the digital channel does not provide the familiar cues people normally rely upon, people can be at risk of making poor trust decisions and placing themselves in harm's way.

29. As well as risks to individuals there may also be societal risks, unwanted changes to the way society works and the social environment people then experience. For example, having greater visibility into the lives of others might lead to polarisation in society, or drive some members of society to be less tolerant of the behaviours of others, or to behave more threateningly to others (as happens occasionally to celebrities).

30. People's attitudes are changing. We should be careful to focus our attention on those harms which remain properly a concern to people after allowing for attitudes to have changed.

There is still a lot more work to be done to understand better the ways people can suffer harm in the digital world.

People's Understanding and Attitudes to Risk

Digital world risks are different in some ways from physical world risks. People's experience recognising and dealing with risks has been developed growing up in the physical world. These experiences might not serve people well in the digital world.

31. The Internet is a multi-generational environment

    - A generation that doesn't know
    - A generation that doesn't care (all new generations rebel against what they see as inappropriate constraints on self expression)
    - A generation that is wired differently because they have grown up since the Internet and PCs became widespread.

    The first generation has only a simple understanding of technology and of how their ICT or personal information can be used against them. They don't know well what to expect from their ICT usage so they can't tell reliably which acts are risky and which are safe.

    The second generation knows more about digital technology and about the dangers but don't believe they can be seriously harmed. They are enthused by the benefits of living in a digital world and confidently expect to take any downside in their stride when and if it happens.

    The third generation doesn't yet know that the digital world is less mature than the physical world and that there are still issues to be worked out. They are at risk of being let down by their naiveté in a world that is still somewhat unsafe.

32. Just because people sometimes act unsafely doesn't mean they don't realise there are risks or that they don't care. Many people find risk a difficult concept to work with because of its uncertainty. Typically, people find it hard to believe in the reality of risks until they see them materialise in a

way that affects them or people close to them. As a result, people often do not make personal risk decisions well. Example: people sometimes turn off an alarm if the alarm gets in the way.

33. People find it easier to imagine possible adverse outcomes and the harms those outcomes could cause. They find it harder to estimate how likely types of outcome and harm really are. People can overstate harms or focus on highly unlikely risks or ignore likely risks.

34. Understanding the reversibility of outcomes is important to understanding people's willingness to accept risks. If the possible outcomes of an activity are feasibly reversible, then people have the ability to back out of the consequences of their actions. They might then be prepared to take risks. In cases where the possible outcome is not readily reversible, people will be much more cautious.

35. Tracking research shows that people tend to be concerned most about the things they believe can cause them serious harm in their lives (crime, health failures, unfair treatment, terrorism, loss of autonomy or freedom of speech, environmental issues, unemployment).

36. People tend to expect their government to protect them from risks that are not entirely within their personal control. People vaguely expect that their government provides a 'guardian angel' to look out for their interests, and that safeguards exist to protect them from the majority of harms. Protecting personal data is high on the list when people are asked.

Setting Out – Vision and Perspective

To make useful progress, we need to start with the right perspective, and to develop a vision of the destination we would like to reach.

37. Consider the roads analogy as one way to describe the destination:

- Roads carry a wide variety of vehicles serving a variety of different purposes;
- Roads are built for safety (vehicle movement is channelled into lanes, crash barriers prevent cross-over, non-skid surfaces increase control resilience under stress) and have safety-specific functionality built in (traffic lights, speed limits);
- The vehicles that run on the roads are built for safety too. Vehicles have safety as a fundamental aspect of their design (the fuel tank is kept apart from the engine), they incorporate safety features (shatter-proof toughened glass, crumple zones) and include safety-specific functionality (seat belts and air bags);
- Vehicles are tested periodically for safety effectiveness (through the annual MOT);
- Drivers are responsible for basic daily safety maintenance (keeping tyres inflated to the correct pressure) and small-scale repairs to safety functions (replacing broken bulbs);
- Drivers have access to 3rd party support services that can address more substantive break-down needs (rescue services, repair garages);
- There is an agreed code of practice for good driving (the Highway Code) and people are expected to be familiar with its principles;
- People are accountable for how they drive every time they take charge of a vehicle, and are personally liable for any harm they cause;
- There are emergency services on call for when serious harm occurs.

For the purpose of analogy, replace vehicles with ICT systems and roads with the Internet. Personal data serves as the fuel that powers the systems people use. In this analogy, the desired destination is a digital world in which the Internet and ICT systems are each built for safety, there are well-understood codes of practice for all participants, people understand their responsibilities and know well enough how to maintain their own safety, and the support services people need are just a telephone call away.

38. The roads analogy might be suitable for the future once the digital society has reached an advanced level of maturity. Maybe a better analogy for the less mature digital society which features in our more immediate future would be the school playground:
    - Children run around in all directions maintaining only localised order (such as on the hopscotch ladder);
    - There are a few general safety rules to prevent serious damage (no pushing someone else off the climbing frame);
    - Playground monitors enforce minimum standards of acceptable behaviour (no bullying or fighting);
    - Otherwise, children are allowed to explore through play what things they like and what things hurt;
    - Each school has a First Aid monitor to attend to cuts and grazes.

    In this analogy, the playground describes the digital world as most people currently experience it, with its limited order and people learning primarily by experience and from mistakes. The short-term destination would be to identify a small number of general safety rules to help people avoid serious damage, and develop a network of 'First Aid' monitors to help people when they do suffer routine problems.

39. Or is the best analogy somewhere between these two? Perhaps the secondary school chemistry lab, where pupils are given the opportunity to handle dangerous chemicals under a set of safety guidelines and are trusted to behave sensibly rather than stupidly? In this case, the destination would be to develop the safety rules for handling personal information, provide people the opportunity to see what safe behaviour looks like before they try it out for themselves, and to have others be ready with a fire extinguisher just in case there is a big accident.

40. From the start, some risk is unavoidable, maybe even desirable, and has to be allowed. Otherwise there would be no learning or progress in the digital world. 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. People will learn from experience how to look after their personal information.

41. Today's younger generation is growing up within a very different environment from that their parents grew up in, an environment in which the Internet, social networking, mobiles, IM, Twitter, on-line games, Google, etc. all have a central role. Each older generation faces this. It is natural for the already grown up generation with their well developed experience and understanding of the last decade to be fearful of the harms they see arising in the next decade and to react against those harms, trying to protect the younger generation for their own good. However, whilst protecting the younger generation from extreme harm, they should not try to stand in the way of progress. Imagine if someone had described a future of motorways and millions of non-expert drivers driving hard metal boxes at high speed in every direction back in the days when people knew only cobbled streets and horse-drawn vehicles. People would have reacted with great horror, no doubt, at the potential for so many people to be caused so much harm, and with disbelief that such a dangerous future could ever be made safe. Similarly, with the explosion of promiscuity in the 60's. Societies develop ways to make potentially dangerous behaviour safer rather than prevent potentially dangerous behaviour from taking place.

42. We should try to develop a suitable vision of the desired destination, of what a future digital society might look like and how potentially dangerous behaviours can be made safer. We need to acknowledge the learning processes through which people adapt to new contexts, situations and threats. And we need to avoid standing in the way of progress.

Setting Out – Approach and Principles

If we are to take pro-active steps to make the future safer rather than simply adopt a laissez faire approach allowing digital developments to take their own course, what principles should inform the steps we take?

43. It is normal practice to presume that the marketplace alone will not cater for all the risks. People will not chose to buy 'the safe option'. Safety is just one of a number of desirables people will trade off when making purchasing decisions. And, like Dr Faustus, when trading benefits for risks people will often choose to take a certain benefit today overlooking that they might have to pay an uncertain or unspecified cost some time in the future. Hence, the market has a tendency to ignores risk, meaning that it encourages risk acceptance rather than risk mitigation.

44. If people don't value their privacy more than they value the benefits they might get by allowing the state and private sector companies greater visibility into their lives, they will lose even more of the privacy they are currently afforded. There will always be opportunities for people to trade away another slice of their privacy for some additional benefit. Hence, under market dynamics the level of privacy provided will inevitably fall to the lowest level sustainable.

45. Possibly we are there already. What we have today is sometimes described as a 'tick-box' mentality, where people are asked to tick the box to show they accept the policy or small print, and where the only options are 'all' or 'nothing'. It is hard to imagine a more simplistic unsophisticated approach to privacy.

46. However, maybe this view of the marketplace does not do it justice and perhaps in time the marketplace will provide the safety we would like to expect. The marketplace is multi-faceted rather than simply one-dimensional. It is capable of doing more than just ignore risk.

    - Insurance makes risk visible and puts a price on it. Hence, insurance is one way the marketplace can cater for risk and can influence people towards safer behaviour.
    - eBay provides a democratic way of rating buyers and sellers, giving people a way to perform personal risk mitigation.

47. Are there other market-based techniques that can encourage risk mitigation rather than simply risk acceptance? Especially, what techniques will work to encourage risk mitigation when other market pressures are pushing towards reduced safety? How could the market drive competitive organisations to provide privacy in cases when there are disadvantages to the buyer (e.g., reduced convenience) as well as disadvantages to the provider (they might be restricted in what they can offer)?

48. If the guiding principle is to find the right balance between risk acceptance and risk mitigation, where does that right balance lie? Should we aim for a situation where systems will give people "the privacy they deserve", whatever that means? How much privacy do people deserve in the current climate, and how do we balance the value of privacy against the value of other benefits?

49. If the guiding principle is most of the time to stand back, providing protections only against extreme harms, what constitutes extreme harm? When potential outcomes and harms can be severe and irreversible, does that provide sufficient justification for stepping in and making it difficult for people to put themselves at such risk? Just as a primary school would be criticised if its playground climbing frame was tall enough a child could easily break his neck in a fall, or the secondary school would be criticised if it allowed pupils to handle explosives strong enough to level the entire building, shouldn't we be criticised for failing to take digital safety seriously enough if we did not try hard to stop people knowingly taking severe and irreversible risks?

50. In the 1950's, pregnancy outside marriage was considered a severe and irreversible disaster. It is far from so today.

51. It is hard to imagine a solution in which people are not expected to take some responsibility, if not the lion's share of responsibility, for their own digital safety. Responsibility for safety will necessarily be distributed with different parties having a different share of the pie, and people as individuals will be expected to take their share of responsibility for keeping themselves and their personal information safe.

52. However, getting people to accept their share of responsibility is not easy. The more safety is built in to the infrastructure and components people use, the more some people will ignore their individual responsibility to mitigate their remaining risks. There is a 'moral hazard' at play. Despite the use of car seat belts being required by law, airbags were brought in because enough people still didn't take on responsibility for their own safety.

Making Progress – Governance

Understanding who the stakeholders are and their interests, the roles and relationships involved, and who has what responsibility authority and accountability, has to be part of the foundations on which any successful solutions will be built. If we don't have a governance framework covering these aspects, we will find it difficult to address the risk issues effectively.

53. For example:

- Who owns the personal information contained within user-provided content sites such as Facebook, YouTube and Twitter?
- Should social sites where there is no charge to the user be treated just the same as a commercial service site? If social sites do not have a commercial responsibility to their customers, do they instead have a social responsibility to their users (e.g. to build in appropriate controls and safety features)?
- Who owns the personal information contained within a government system? For example, does the Secretary of State for Health own a person's medical data, or does the person themselves own them?
- When does consent become informed consent? Is a 3rd party fulfilling its responsibility to the user by stating in the small print somewhere what might be done with someone's personal data, or should the requester of consent be required to inform and explain everything the person might need to know in plain uncluttered English?
- How can accountability be enforced across jurisdictions on the Internet?
- If users are responsible for their own safety, who is responsible for explaining that to them and providing them with the tools they might need?

54. In some ways, a citizen/government relationship is different from a consumer/provider relationship. The government is not simply a provider of a specific type of services. It has supervisory responsibilities (placing bounds on authorised behaviours, enforcing safety requirements). It has monopoly powers and it has coercive powers, and it has unique authorities and capabilities. Some arms of the state have the authority to gather the data they need for their purpose by compulsion, without requiring the consent of the individual data subject. Patterns or principles, such as the principle of data ownership, might work one way in a commercial relationship but not in the same way in a government relationship.

55. Any governance arrangements developed will need to reflect the nature of the relationships between people and the state and between consumers and providers (e.g. the asymmetry of authority and capability) and to provide controls and safeguards to protect people's interests in the face of the limited capability people have to protect themselves once their information is beyond their immediate purview or control.

Making Progress – Controls and Techniques

Cars are physically hard objects, can more around at speed, and can generate very high levels of deceleration if they hit something suitably solid and inert. They can momentarily veer out of control if they get a puncture or if some moving part breaks. As a result, cars have safety functionality (e.g. powerful brakes) and they have safety features (e.g. crumple zones, toughened glass). What are the equivalent safety functions and features needed of the ICT structures and systems that handle personal data?

56. Is the familiar approach of limiting access to data (locking data away so it cannot be misused) the right approach for personal digital systems? If a person's information is out on the Internet already then access controls can't be used to control what people might do with that data. The ideas and metaphors for assurance might need to change. We need to find other ways to control data use besides preventing access.

57. The UK's roads carry pedestrians, bicycles, private cars, public transport vehicles, and heavy goods vehicles, all of which share the same infrastructure. Similarly, the Internet has private personal systems (e.g. social networking sites, video content sharing sites), public personal systems (e.g. how-did-i-do.co.uk, which has information specific to named individuals that is not considered sufficiently personal it needs to be restricted), and service systems (which could be private sector or public sector systems, providing commercial or social services to consumers or citizens). Is it instructive to classify personal data systems in a way that parallels how we classify road vehicles (private car, private hire car, passenger vehicle, heavy goods vehicle) and would we then have different rules and guidance for different types of system (e.g. a central government civil servant using a public sector service system needs the equivalent to an HGV licence whereas a private sector system provider needs only an ordinary driving licence; private sector systems are subject to spot checks at any time whereas private personal systems need only an annual 'roadworthiness' test)?

58. Experience shows that there are situations where 3rd parties use personal data in ways that might seem acceptable or justified to them but that are seen by the information subject as contrary to, or at least not responsive to, their best interests. This is one of the charges sometimes made at organisation-centric design as opposed to person-centric (or user-centric) design. Should person-centric design techniques be encouraged for personal data systems and organisation-centric design discouraged?

59. How does one stop organisations flouting the rules for the protection of personal data? There is no excuse (other than a past lack of enforcement) for systems not to be "street legal" today. The relevant legislation (the DPA) has been in place for over 20 years.

60. Are there other means to achieve enforcement besides policing by exception? Policing by exception should be part of a multi-track rather than single-track approach. Build secure and sensible systems, educate and inform users, and encourage users to challenge the exceptions they come across.

61. The DPA's principles are largely unchanged 20 years on. The DPA was created in response to the worries people had about privacy back in the early eighties, and that was before the Internet and PCs became widespread. The risks are different in nature and magnitude today. Technology is freeing us from the requirement to know where data is held before we can use it. We need to update the Data Protection Principles in recognition of the changes which have taken place and to bring them into the 21st century.

62. Perhaps we need Data Protection Rules as well as Data Protection Principles (just as we have traffic lights for busy road junctions when 'right of way' principles on their own might not be sufficient). What might Data Protection 'traffic lights' look like and where would we put them?

    - Traffic lights might take the form of explicit acknowledgements, auditable records, review and accountability;

- Placement might be where the interests of parties conflict rather than simply diverge.

63. Can we expect pro-actively to identify what constitutes good safety and security practice and develop Codes of Good Digital Practice without having to wait for people to be hurt first?

64. Can we perhaps use a 'penetration testing' type of approach where under controlled circumstances we have people try to exploit the very problems we seek to advise about to demonstrate in a safe way the risks that need to be avoided and the vulnerabilities that need to be addressed?

65. Educating the user doesn't, on its own, address the whole problem, but it does help and should be considered one part of the solution even if it is not all of the solution. However, educating the youthful user is a challenge. Youngsters are often unresponsive to advice and guidance from people outside their milieu (with the exception being primary school teachers who do have the ability to influence and educate the young as they can catch youngsters young enough they will listen and early enough they are unlikely to have already put themselves in harm's way). The adults best placed to have influence over the behaviour of digitally active youngsters are those within the milieu, i.e. the owners of the components (Microsoft, Google, Facebook, EA Games). Perhaps these organisations should be charged with providing appropriate education to people?

66. The media can be successful at raising issues and educating people (see how *The Independent* raised the issue of the use of tips in restaurants). Perhaps the media too should be used to provide education to people?

67. However, we would need the information provided (whether by the media or otherwise) to be good quality information consistent with other good advice. We would need meaningful information (e.g., real-world statistics presented in a personal narrative) about what can and does happen to people who find themselves affected by digital harms, not sensationalism.

68. Regardless of the effort placed on the education of people, we need to maintain a strong focus on prevention. If people can do insecure things they eventually will do insecure things and will keep doing it as long as nothing bad happens (that they know of). Security awareness is best left for all the places where preventative controls do not exist.

How should we respond? Should we educate children about digital safety in primary school? Should we educate the parents of those children first? Should we form NGOs to bring pressure for responsible change on component providers such as Facebook and Google, and on infrastructure providers such as ISPs? Should we aim to advise policy makers, regulators and legislators?