

The Proportionate Sharing of Personal Information

Results from IAAC's PCIA Workshop of 16 February 2010

Introduction

There are many areas within the operation of government where people's personal information (PI) is gathered and shared for public interest purposes. In many of these situations, decisions by the bodies that hold PI on whether or not to share someone's PI with another government body are quite simple. These include situations where the public interests being served by sharing can safely be assumed to be aligned with the personal interests of the people whose PI is being shared. For example, when someone's change-of-address details are shared across a range of government departments, the public interest in the efficient administration of services is in line with the individual's presumed interest in reducing the inconvenience of having to give out the same information repeatedly.

However, there are also many situations where decisions on whether or not to share PI are more difficult. These include situations where the public interests behind sharing requests are potentially in conflict with the personal interests of the individuals involved. One example is when data about people's Internet browsing or phone call traffic are made available to the security services. The public interest in preventing terrorism is in contention with individual people's private interests in maintaining their autonomy and not being implicated unfairly by their association with other people. In these situations, non-trivial decisions have to be made by PI custodians regarding whether it is appropriate for the requested PI to be made available, in part or in full, to the requesting party. Bodies that are custodians of PI have a duty to ensure that the PI sharing decisions they make are decisions the public at large will accept.

The objective of this workshop was to explore how people feel about the sharing of PI, and to suggest what this might mean for custodians of PI when sharing requests are made to them. The particular focus was on how public sector bodies (PSBs) can build and maintain the public's confidence in their PI sharing decisions in those situations where sharing PI might be in the public interest but is potentially not in the personal interests of the individual people concerned.

Disclaimer: This report is not intended to serve as a record of the workshop discussion. It is, as with previous workshop reports, a digest of the many insightful points made in the discussion. The ideas expressed in this paper should not be taken to represent the views of any individual IAAC member or sponsor.

Key Messages

1. Current PI gathering practices are far from perfect, exposing a degree of limited understanding and muddled thinking behind some of the information gathering practices people are currently exposed to. This gives rise to a number of concerns people have when asked to provide PI to public or private sector organisations.
2. With regard to people sharing their PI with the private sector, people feel they have some tools with which to manage their concerns. They feel they have some control over the sharing process, that several safeguards exist to protect them, and that they would be able to obtain redress should they be wronged. With regard to sharing with the public sector, the situation is quite different. People do not feel they have the same level of control or protection. Instead, they feel they have little option but to trust the PSBs that handle their PI. This puts an onus on those PSBs to provide adequate safeguards and to take care not to abuse that position of trust.
3. There are two decisions a PSB needs to make when considering how to respond to a sharing request. The first is a binary decision: is sharing permitted or not? If it is, then the PSB needs to consider the second decision. That is a proportionality judgment: is the requested sharing appropriate?

Registered Number 432637

Sponsors:



4. Proportionality judgment calls are normally made on a case-by-case basis. They can be complicated, and there are few if any published guidelines available to help PSBs come to their decisions. Having guidelines available would clearly be of benefit to PSB decision makers. Publishing those guidelines would help to promote public confidence in the PI sharing that does take place.
5. Consent and transparency are both essential to building and maintaining the public's confidence in the sharing that takes place. Both of these have a history of causing PSBs some difficulty and people do not feel that they are currently provided with adequate options and mechanisms. This IAAC report provides a number of ideas that might help PSBs to overcome these difficulties, including the idea of consent minimisation as a way to improve people's trust much as data minimisation improves people's privacy.
6. There are a number of areas of research that could be undertaken to aid the development of publishable PI sharing guidelines. These are identified in this report. They include building on a number of ideas that have been developed in the context of Freedom of Information.

Discussion

The relationship between people and the public and private sectors

People feel that the situation they are in when sharing their PI with the private sector is somewhat different from the situation they are in when sharing PI with the public sector. They feel that they are on firmer ground when dealing with the private sector.

Sharing PI with the private sector

1. With regard to sharing PI with the private sector, the situation is relatively straightforward. Each instance of sharing can be thought of as a discrete value exchange between two parties for a specified purpose. Often it is a value exchange that the individual themselves has initiated, such as when they register as a user of a service or website. The individual is likely to have a general understanding of what information is needed to fulfil the purpose being served and hence of what PI it is appropriate for them to share. In return for sharing certain of their PI and granting limited permission for its use, the individual receives a specified benefit they are seeking.
2. For example, people are generally aware that it is advertising that enables services such as search services or social networking services to be provided free to the user. The value exchange being made in these cases is that the individual gets access to a service they want in return for consenting to the limited use of their PI and to receiving targeted advertising.
3. People tend to feel they have choice and therefore some power in the sharing process, even if their only choice is to walk away from an unfavourable exchange and transfer their 'business' to a different provider. They also tend to feel they have some protection in the process. This might be a vague feeling of protection, as in a faith in an unspecified 'Guardian Angel' looking out for their interests, or a specific feeling as in believing in the sufficiency of the particular safeguards of which they are aware.
4. People can be described as having a wary scepticism with regard to how the private sector uses their PI.
 - They assume and accept that, within reasonable limits, private sector companies will try to get the most they can out of the PI people share with them. The pursuit of lawful profit from the use of PI is accepted as fair.
 - Private sector companies are presumed to be operationally competent. This extends to the company and its staff being competent at protecting customers' PI.
 - Companies are expected to look after the PI they hold and to use it only as permitted. They are expected not to share that PI with others unless expressly permitted to do so, and not to use that PI for other purposes unless expressly permitted.

Registered Number 432637

Sponsors:



- People feel somewhat sceptical that the self-imposed restrictions claimed by private sector organisations in privacy policy statements are actually honoured in reality. To some degree, privacy policy statements are seen as promises that are honoured whilst they remain convenient but available to be broken when they become inconvenient.
- People generally believe they would be able to obtain legal redress if their PI were misused to the extent that they were subsequently wronged (their rights infringed, or they were caused disadvantage or harm).

Sharing PI with the public sector

5. With regard to sharing PI with the public sector, the situation people generally feel they are in is somewhat different.
6. The sharing transaction can still be seen as a value exchange but in these cases the exchange is much less straightforward.
 - People see local government and central government each as a collection of closely connected entities. They expect information to flow from entity to entity within each level of government and to be used by those entities in various different ways for various different government purposes. Hence, instances of sharing tend not to be thought of as discrete exchange transactions. They are seen more as part of a series of exchanges taking place under an enduring relationship between the person and the public sector.
 - Each exchange is as likely to be initiated by the public sector body seeking the information as it is by the individual seeking a service or benefit.
 - The benefits people get from the public sector can be less tangible than those provided by the private sector (e.g. greater public order, better safety and security) and can be indirect benefits to the community or society as a whole rather than direct benefits to people as individuals.
 - People are likely to have less of an understanding of what information is needed for any particular purpose being served and hence of what PI it is or is not appropriate for them to share.
7. People do not feel they have much choice, or that they have the level of influence or control over public sector bodies that they have over private sector bodies.
 - People do not feel they have much choice: they might on occasion be able to choose not to cooperate with an individual PI request but, for most public sector services, they do not feel they have the choice of terminating the relationship and transferring to a different provider.
 - People do not feel they have much influence or control: they realise that some functions of government can proceed without requiring their explicit consent and that those functions would not work if the situation were otherwise. People have at best a tenuous community influence over the public sector (based on their ability to complain or protest en masse) rather than personal control based on explicit individual consent.
8. People can be described as having fragile conditional faith in how the public sector uses their PI.
 - Conditional faith suggests that, on the whole, people tend to start from a position of trust, presuming the public sector looks after and uses their PI properly, provided there are no indicators to the contrary.
 - People tend to accept the use of their PI for public interest purposes as fair, regardless of the particular public interest being served.
 - People tend neither to demand nor expect as high a level of competence of the public sector as they do of the private sector.

Registered Number 432637

Sponsors:



- Public sector organisations are expected to look after the PI they hold and to use it only within limits. However, these expectations are weaker and the limits are looser than with the private sector. People expect that there will be some sharing going on in the background, that their PI will be used in some ways without their consent, and that a level of mistakes and errors will occur.
- People feel that there is the potential for the harms they might be caused by the public sector's use of PI to be more substantial than the harms they could be caused by the private sector (this is not the same as saying that they expect the harms to be substantial, just that they feel the potential is there).
- People feel less sure about the protections they would be afforded if they were wronged by the public sector. Whilst people appear to trust that in most situations the safeguards they hope are in place would prove effective if called upon, they suspect there can always be some situations in which the safeguards would prove to provide only limited protection against central government use of their PI. They cannot be sure avenues will always exist to enable them to right any wrongs they might be caused.

Current information gathering practices

How might people characterise the information gathering practices they are exposed to?

9. People have a general sense that many of the practices by which PI is handled today are poor, reflecting a generally poor understanding of the role information plays in many activities and of the different values of different types of PI. There is a degree of muddled thinking behind some of the information gathering practices people are currently exposed to. People, whether as individuals or as officials, do not always appear to understand well why the requested PI is being gathered, how it will be used, what its value is, and what controls it is expected or required to be under.
10. Sometimes it seems that more PI is requested than would appear justified by the ostensible purpose. This might be because the purpose is not made clear, or because of muddled thinking. It gives rise to suspicion that there is an unstated purpose being served in the background.
11. Sometimes it seems that PI is gathered speculatively. PI is gathered even if there is no clear need for it on the basis that there might be a need for it in the future. This might be because it is felt easier to gather all the PI that might be needed at the same time than to make separate requests for different PI as needs emerge.
12. Sometimes it seems that PI is gathered defensively, to protect the gathering organisation's reputation rather than to provide a benefit to the individual. This relates primarily to the public sector. PSBs are expected to provide services that fall within their remit. They are also, to some degree, expected to keep a look out for the citizens they deal with and to protect those people from possible harms that could arise. PSBs are then vulnerable to being criticised, fairly or unfairly, for not having had the foresight to gather information that might have enabled them to prevent a harmful outcome from happening. As a result, PI is sometimes gathered from people not because it is needed for the provision of services but because it might prove relevant to protecting the individual in some unspecified way.
13. Many people feel that current practices for seeking consent are poor.
 - They often feel that they are not given a fair and free choice when asked to provide consent. Policy statements can be excessively long, challenging to read, and written more to protect the organisation against the individual than to protect the individual from the organisation. These leave people without a clear understanding of what processing restrictions would apply if they were to give their consent. From the point of view of the individual, the consent being sought might just as well be for the unrestricted use of their PI.
 - In other cases the consent being sought might be clear but still appear to be broader than the limited consent needed to enable the person's stated needs to be met, and only one 'take-it-or-leave-it' consent option is offered. This means that if the person wishes to withhold their consent to the overly broad use of their PI, they cannot do so without the whole process they are engaged in coming immediately

Registered Number 432637

Sponsors:



to a halt. In these cases, people can feel that the gain they are seeking is being held hostage to them providing broader consent than they feel comfortable giving. The request for consent does not appear fair, and the consent they give is not given freely.

People's decision process

How do people decide on providing whatever PI is requested?

14. The decision process people follow is often fuzzy, leading to them making unsettled decisions. It is also partly, if not largely, subjective and context-specific. This leads to individual people coming to different decisions for the same PI when circumstances differ, and to different people coming to different decisions for the same PI when the circumstances are much the same.
15. The sharing decisions people make can be largely subjective.
 - Some people describe the personal details other people post onto social networking sites as “intimate”, suggesting they do not consider them appropriate for sharing, whereas other people see those same details as “part of who they are” and are happy for those details to be in the public domain. This suggests different people have different views of the value of some items of PI, primarily of the possible disadvantages or harms that could arise for them, as well as of the potential benefits that people might get from posting such data.
 - The weight people give in the decision process to the value of the potential gain being served by sharing varies depending on the nature of the gain. Assessments of value, direct or indirect, can be highly subjective.
 - Where the gain is a direct benefit to the individual, the value of the benefit is usually clear to that individual and it plays a significant part in that person's decision process. That value can vary widely. People will sometimes trade their PI with only low regard for the relevance of the information requested or for the possible risks of sharing it if so doing unlocks an immediate benefit they are eager to access.
 - Where the gain is indirect, as can occur in public sector exchanges, the value of the gain tends to play a less significant part in the decision process. People do not tend to differentiate between different public interest purposes on the basis of their value, and tend to accept the legitimacy of a sharing request whatever the public interest being served. Even if people are uncertain as to the relevance of the PI requested to the stated purpose, people's sharing decisions are unlikely to be changed by those doubts. They might rationalise sharing PI of unclear relevance by saying “well, they already have that information anyway”.
16. The sharing decisions people make are usually context-specific.
 - The PI concerns people have are based on their fears of the possible harms they might conceivably suffer. These reflect the particular circumstances of the exchange as well as the category or nature of the PI they are being asked to share. Hence, people might agree to share particular PI in some situations but not in others.
 - If the PI is subjective (e.g. GP comments within medical records), then people might well have different feelings about its use and sharing than if it is objective (e.g. information relating to a criminal record).
 - If the PI is objective information, then, assuming it is correct, the person cannot deny being associated with it and they have to accept any disadvantage or harm that comes with the fair use of that information. If objective PI is incorrect, it can be shown to be incorrect and can be corrected.
 - If the PI is subjective information, the person may or may not agree with what that information says about them. However, even if they do not agree with it, the person can still be harmed by it.

Registered Number 432637

Sponsors:

As a result, they might consider any sharing or use of that subjective information to be unfair. If the PI is incorrect, they might have difficulty convincing others that it is incorrect, making it harder for them to obtain remedy for unfair consequences.

17. The sharing decisions people make can be fuzzy, leading to them making unsettled decisions.
 - When people think about the possible harms that might befall them, they naturally think first of uncommon extreme potential harm events before they get round to thinking about more common less extreme potential harm events. As a result, people's initial reactions to sharing might be based on a fear of unlikely or unrepresentative outcomes whereas their more considered reactions might be more moderate. People's initial decision might be to object to sharing but when pressed, they might step back from their initial objection and decide that "maybe it is alright to share that information after all".
 - Even if a person cannot immediately articulate a particular harm they might fear, that does not stop them feeling anxious about the possibility that harms might arise. The potential for harms to arise will influence how they feel about sharing even if they can't put into words a credible example of a harm that might realistically arise.
 - In the absence of direct personal experience of harms, people's awareness of issues and their attitudes towards sharing can be influenced by reports in the media. Media reports tend to emphasise extreme and unrepresentative events, supporting fears and making it more difficult for people to progress to a more moderate and considered decision.
18. In summary, people feel they are on firmer territory when dealing with the private sector than with the public sector, the particular information gathering processes they are exposed to are far from perfect, and their thinking about sharing is not straightforward. The net result is that, in many situations, people are sharing their PI even if they feel a little uncertain doing so. With private sector sharing, people feel they have some tools with which to manage their concerns: the situation is relatively simple, the potential benefits are often clear, each individual exchange is seen as discrete and to have only a limited potential to cause harm, people feel they have choice and some control, people feel there are safeguards in place for their protection, and people believe they would have recourse should they be disadvantaged or harmed. With respect to the public sector, all these aspects are different. With public sector sharing, people often feel they have little choice but to trust the public sector regardless of the situation.

Organisations' current information sharing practices

Given the above description of how people generally feel about sharing their PI, what sharing practices do organisations have in place today and how could these be improved? We shall look first at current sharing practices.

19. There are two decisions an organisation needs to make when considering how to respond to a sharing request. The first is a binary decision: is sharing permitted or not? The second is a judgment call: is the requested sharing appropriate?

Private sector sharing

20. The primary requirement for private sector organisations is that they stay within prescribed legislative boundaries.

1. Is sharing permitted or not?

21. Legally, sharing is permitted if it is in support of a legitimate purpose (a consented purpose or one covered by a contract freely entered into).
22. Sharing is a form of disclosure so the sharing of PI is covered by the Data Protection Act (1998). It is also covered by the Human Rights Act (1998), primarily the right to respect for one's private life and the right not to be discriminated against in respect of one's rights and freedoms.

Registered Number 432637

Sponsors:



2. Is the requested sharing appropriate?

23. People tend to feel that sharing needs to be fair for it to be considered appropriate.
24. Within the terms of the Data Protection Act, fairness is based primarily on transparency: say who you are, what you will do with the information, what safeguards exist, how people can object.

Public sector sharing

25. The primary requirement for public sector bodies is not only that they stay within prescribed legislative boundaries but also that the decisions they make should be ones the public can accept.

1. Is sharing permitted or not?

26. There are a number of steps PSBs should go through to ascertain whether the requested sharing is permitted.
 - The first question is whether the sharing is lawful. Is there a statutory requirement to share or a blanket permission to share, and is the sharing consistent with relevant legislation (e.g. the Data Protection Act, the Human Rights Act)? The DPA recognises that there are public interest grounds for data sharing that exist outside the frameworks of consent and contractual legitimacy. There are also exemptions within the Act that create legal frameworks for the secret sharing of data.
 - The second is whether the sharing is legitimate. Is there a valid operational reason to share (such as sharing in support of the PSB's responsibilities under relevant acts of parliament, or sharing in the public interest)?
27. PSBs should gather subject consent where they can (e.g. on relevant forms). However, there are many situations in which non-consensual sharing can occur, for example when information is requested by the intelligence services or SOCA.
28. PSBs must have adequate security measures in place to prevent the inadvertent sharing or disclosure of PI. These should be measures the public can have confidence in. For example:
 - They should follow a principle of data minimisation: share the minimum data needed to support the purpose, and have the default be no sharing.
 - They should implement strong security measures to prevent or deter unauthorised release or sharing from taking place (e.g. to prevent the loss of data and to prevent staff accessing data they are not authorised to access).
29. Where appropriate, conditions may be imposed by the PI custodian on the recipients of shared PI (e.g. no onward sharing with other bodies).

2. Is the requested sharing appropriate?

30. Proportionality normally has to be decided on a case-by-case basis. These decisions are often far from simple.
31. Legally, for an activity to be considered proportionate it has to be necessary as well as being permitted. It is not sufficient that the activity is just a good idea. However, necessity is a more subjective test than either of the tests for permissibility (lawful or legitimate).
32. Being judged legally as necessary is itself necessary but not sufficient. Legal principles endeavour to reflect the morality of the day within society, though by necessity they often lag some way behind. Morality (people's beliefs and expectations about what is right) leads the law. An activity might contravene a long-standing piece of legislation but public attitudes might have changed such that people no longer see that activity as wrong. As a result, legal practice recognises the need for latitude in the interpretation of statutes

Registered Number 432637

Sponsors:



to accommodate the ways in which people's expectations and opinions about right and wrong might have changed.

33. Judgments of current morality can be complicated and fraught. What is currently considered morally right is a matter of aggregate attitudes and opinions, and morality within a society is neither uniform nor coherent. The leading edge of change can head in many different directions.

How might current practices be improved?

34. Given the concerns people have about how their PI is gathered and used, and the complexity of many proportionality decisions, the goal should be to have sharing practices be put on as firm a basis as is possible and for the public to have every confidence in the sharing decisions that are made. PSBs should aim to make their proportionality decision practices and relevant safeguards as strong as they reasonably can be made. This would help people to feel confident that PSBs are not abusing their position of trust, and would help to build public confidence in the sharing decisions made.

Consent and Transparency

35. Consent and transparency are both essential to building people's confidence. Consent (where needed and sought) implies that any PI use outside the scope of the granted consent will not be undertaken. Transparency provides people with confidence that none other than authorised extra-consensual uses are taking place.
36. Consent helps the individual to trust the organisation that handles their PI, i.e. to trust that the organisation will not make extra-consensual uses of their PI. Despite the importance of trust and the importance of consent in creating that trust, obtaining and staying within the bounds of consent still appears to provide some organisations with a number of challenges.

- Organisations need to make it clear to people what they are asking those people to consent to. Descriptions need to be brief, in plain English, and accurate.
- Just as the principle of data minimisation serves to strengthen privacy protection, organisations should adopt the principle of consent minimisation to strengthen trust.
 - Consent should be specific and permit only those uses that are necessary. Asking for broad non-specific consent undermines what trust might exist between the person and the organisation.
 - Consent should be retained for only as long as it is needed. In some situations, consent needs to be enduring, but in many others it does not, and in those cases it should be limited to the needs of the specific purpose being served at the time. If that purpose arises again at a later date, fresh consent should be sought then. Organisations should not presume previously obtained consent can safely be resurrected.
 - Consent exists within a trust relationship. This means that consent is not transferable. A person might consent to one particular PSB making use of their PI but this does not mean that they would consent to other PSBs, even those within the same level of government, making use of their PI. Fresh consent needs to be sought by each PSB.
- To be meaningful, consent should be given freely in response to a fair request. If the consent requested is specific and explained clearly, people are likely to understand that withholding their consent will result in the impairment or termination of the process under way and that it would be only fair that they would then not be able to obtain in full the gain they were seeking. They would then be able to decide accordingly. If the consent is non-specific or poorly explained, people are likely to feel that the gain they are seeking is being held hostage to them providing broader consent than they feel is necessary or that they are comfortable with. In such cases, the request for consent would not appear fair and any consent given could not be considered to have been given freely. Trust would, again, be undermined.

Registered Number 432637

Sponsors:



- Consent, once provided, needs to be honoured for the duration. Function creep is a particular danger, and organisations need to be vigilant that function creep does not lead to information gathered for one purpose being used subsequently for another purpose in violation of (implicit or explicit) consent.
 - People need to be able to revoke consent. People can change their mind, perhaps because they have acquired a better understanding of relevant topics or perhaps in response to events experienced or reported in the media. Requirements for the revocation process need to be understood and convenient mechanisms for revoking consent provided.
37. Transparency is an essential partner to consent. Where consent builds trust in an organisation's intended behaviours, transparency builds confidence in the actuality of how PI is being used.
 38. People generally do not feel that they are offered adequate transparency, and feel transparency mechanisms should be strengthened.
 39. Transparency should not be equated solely with the disclosure of what PI data are being held by organisations. People knowing what information an organisation holds about them is important but it serves little benefit if they do not also know what that organisation is doing with their information.
 40. Transparency should provide people with confidence that the only uses that are being made of their PI are those that are lawful, legitimate and fair. Transparency should identify the range of PI held, the uses that are being made of that PI, and the purposes that are being served by those uses. People tend to accept the use of their PI for public interest purposes as fair regardless of the particular public interest being served. Transparency should, in addition, provide assurances that the stated uses and purposes are the only ones being served.
 41. For transparency to provide people with confidence, it has to be presented in the form of simple, clear, credible explanations and assurances.
 42. To build confidence in transparency claims, organisations should provide reliable audit trails of how PI has been used and of what PI has been shared with which other bodies for which uses and purposes. Audit trails provide substance to assurances that no non-consensual, unauthorised or unfair uses or sharing of PI have taken place, including showing that any conditions imposed by a custodian on the recipient of shared PI have been honoured. Audit trails can also serve to help people obtain remedy or recompense if they believe they have been inappropriately disadvantaged or harmed. Faith in the ability to obtain remedy or recompense contributes to people's confidence in PI sharing.
 43. Some people will wish to be given greater assurances than others might feel they need, and will require more transparency than will others. Transparency mechanisms should be designed to provide everyone with an adequate standard level of transparency and to enable those few who would seek more to obtain more. Giving people subject access rights already provides this flexibility with regard to one aspect of transparency (knowing what PI is held by an organisation). Flexibility should be extended to all aspects of transparency.
 44. As with consent, providing transparency appears to cause some organisations difficulty. Realising that the role of transparency is to build confidence in the uses being made of PI rather than just to disclose what PI is being held might help to solve some of those difficulties. Transparency has traditionally proven difficult to provide in situations where the disclosure of the PI held is potentially in conflict with the public interest being served by that PI (e.g. providing subject access to DWP data, to subjective medical data, to law enforcement data). In many situations, disclosing the uses being made of people's PI and the purposes being served by those uses can be achieved without disclosing the specific content of the PI being held. This would enable the purpose of transparency to be achieved to a large degree where traditionally that has not been thought possible.
 45. Similarly, non-consensual sharing does not have to mean non-transparent sharing. People should be made aware of the situations in which PI can be shared non-consensually even if they are not able to prevent that sharing.

Registered Number 432637

Sponsors:



Security Division of EMC

46. Providing less than full transparency should be permitted only in those (few) situations where the provision of transparency regarding the uses made of PI can be shown to be substantially in conflict with the public interest purpose being served by those uses.

Beyond Consent and Transparency

There are further steps organisations could take to strengthen public confidence in PI sharing practices.

47. Data minimisation – PSBs should follow a principle of data minimisation and both request and share the minimum range of data needed for the specified purpose. This puts a responsibility on the requesting body to specify its purposes and to request only the minimum range of PI data needed for those purposes. It puts a similar responsibility on the custodian of PI to consider the appropriateness of the stated purposes and to provide only the minimum range of PI data needed for those. PSBs should develop standards for common sharing exchanges between them and other bodies.

Where sharing requests can be automated, the requesting body does not need to request all the PI it thinks it might possibly need for future work in the one initial request. Requesting PSBs have the ability to make limited initial requests and to follow those later with further requests if further PI proves to be needed. This might help the current practices of opportunistic and speculative gathering to fall away.

48. Data correction – PSBs should implement mechanisms that allow objective data to be correctable where that objective data can be shown reliably to be incorrect.
49. Remedy and recompense – PSBs should
- implement mechanisms to identify when an incorrect or unauthorised exchange of PI has occurred (e.g. they have been provided with excessive information; they have inappropriately disclosed confidential information),
 - identify the steps they can take to remedy any improper exchanges (e.g. delete the excessive information and report back to the provider; prevent the recipient using improperly disclosed confidential information),
 - address the cause of the improper exchange (e.g. improve sharing procedures; discipline offenders), and
 - put in place mechanisms to provide recompense to individuals who have been affected by improper use or sharing (e.g. assurances that the improper exchange will not recur; compensation for those who have been harmed).
50. Education, training and guidance – PSBs should provide education, training and guidance to all staff who handle PI. This is so staff will understand what PI is needed, what protections and safeguards are needed, what the data subject's rights are, and what their personal responsibilities as PI handlers or custodians are. [The BCS and ISAF released a 12-page *Personal Data Guardianship Code* in the summer of 2009 to help staff who handle PI to understand their responsibilities.] The provision of staff training can also serve to reduce the organisation's liability should an improper exchange occur.

In support of better practices

There are further steps that could be taken, beyond those that individual organisations handling PI should take, that would aid the development of publishable PI sharing guidelines and strengthen sharing practices.

51. PI includes a diverse range of different types of data. PI can include objective data, subjective data, static data, situational data (the type gathered by CCTV), transactional data (e.g. Oyster card records), activity data, and possibly further types of data. Different protections and safeguards might be needed for different types of data. Furthermore, protections and safeguards might need to be applied differently according to the specific nature of the data (for example, subjective data created by a GP might be afforded different protection from subjective data created by a police officer). It might be helpful if research could be

Registered Number 432637

Sponsors:



undertaken to identify each of the different types of PI data possible and to explore the protection requirements and dependencies each type of PI data has.

52. Current practice with regard to making proportionality decisions appears to be in its infancy, with decisions being made on a case-by-case basis with no established guidelines existing in the public domain. This is in contrast to Freedom of Information disclosure decisions where there are a number of published guidelines available relating to how such decisions should be made. It would help to strengthen proportionality decision making if guidelines for PI sharing could be developed. It would help to strengthen transparency and people's confidence in the proportionality decisions made if those proportionality guidelines could be published.

In order for such guidelines to be developed, understanding would need to be improved in a number of areas:

- What counts as being in the public interest when sharing PI? There is not a common or settled understanding of what constitutes the public interest, though this area has been extensively mapped out in the context of Freedom of Information. Though there are differences between FoI and PI sharing (FoI involves contention between two public interests whereas the sharing of PI involves contention between public and private interests) it is likely that much of the understanding that has been developed to aid FoI disclosure decisions (e.g., that public curiosity does not count as being in the public interest) could be applied to the context of PI sharing.
- What is the relative value of different public interest purposes? Again in the context of Freedom of Information, FoI guidance provides a hierarchical grading of the values of different public interests and shows when a specific good (such as the protection of international relations) may trump the general good of transparency and disclosure. Adopting a similar hierarchical grading might help PI sharing guidelines to indicate when a specific public interest good may be used to permit the non-consensual sharing of sensitive or confidential PI, or restricting subject data access, or providing less than full transparency.
- What, beyond being legally permitted and within the requesting PSB's business remit, constitutes a justifiable reason or due cause for requesting specified PI be shared? Alternatively, if this would be the simpler end from which to approach the problem, what would make a sharing request invalid or insufficiently justified for PI to be shared as requested?
- What information does a requesting body need to provide regarding the circumstances, the purpose that will be served and the uses to which PI will be put, to enable the custodian of the requested PI to determine whether a sharing request is justified and to determine the minimum amount of PI it needs to share (e.g. so it can determine that a request for PI should be rejected and remade in the form of a request to confirm or otherwise PI that the requester should already hold)?
- How best can consent granted by a data subject travel with that person's PI when it is shared so the recipient of shared PI can maintain respect for the context in which the PI has been gathered as well as the specific terms of the consent granted?
- What are the respective roles of the various parties involved in the sharing of PI, and how should ownership, authority, responsibility, accountability, liability and reporting be assigned across the various roles?
 - Within normal Data Protection situations, there are three recognised roles: data subject; data controller; data processor. However, when PI is being shared between two processing organisations, there is a transfer of responsibility from one data controller to the other as well as from one data processor to the other. The two data processing organisations might well be using the same PI to serve different purposes and each might be authorised to makes uses of PI that the other is not. Hence, PI sharing might require a different set of roles and/or a different assignment of governance functions between those roles than is normal within more usual Data Protection situations.

Registered Number 432637

Sponsors:



Security Division of EMC

- The meaning of ownership and custodianship, and in particular the rights and responsibilities associated with ownership and custodianship, need clarification. Whilst many people might consider that, in principle, they are the owners of their PI, in the UK the data subject does not have legal ownership of the copy of their PI that has been gathered by government. What rights, authority, control or veto people might expect ownership to afford them over the retention or use of their PI is unclear? Ownership does not have to imply absolute rights. For example, people own their own money and many would assert that ownership affords them the right to decide how their money will be used. However, ownership does not give people the authority to refuse to pay taxes. The state, without the need to claim ownership, is able to assert a superior authority. Likewise, the state should not need to claim ownership of gathered PI, or deny data subjects ownership of their PI, in order to retain the control it believes it needs over the PI it uses. Without clarification, the rights and responsibilities of ownership and custodianship cannot be strengthened and control cannot be assigned appropriately.
53. Consideration should be given to developing a framework giving substantive weight to independent investigative audits. Independent audits that have the ability to uncover PI uses that are being concealed would help to provide the public with confidence that the PI promises made in privacy policy statements were being honoured without regard to convenience.
 54. Consideration should be given to developing a framework of legal protection for organisations and staff that make proportionality decisions. A decision on proportionality involves a judgment of what does or does not appear fair and appropriate. This involves more than just determining what fits within the boundaries of relevant statutes. It requires officials to have a high level of understanding and familiarity with the use and protection of PI, and to use common sense. For that to be possible, officials need to be afforded a defence against prosecution or pillorying for using common sense even if the end result in a particular instance was an unexpected and not reasonably foreseeable adverse outcome, disadvantage or harm. An ombudsman or the courts might be an appropriate way to adjudicate on the use of a common sense defence.

Registered Number 432637

Sponsors:



Security Division of EMC