IAAC Identity Assurance Programme 2008
Report of IAAC's 5 March 2008 Workshop
"Citizen Control"

Summary

IAAC held a workshop on the 5th March 2008 to examine what powers and safeguards would be needed to provide Citizen Control within a national digital identity infrastructure (NDII).

Citizen Control serves to allow the citizen to take additional precautions, in situations where they feel that is needed, to ensure their safety and security when participating with the NDII. It is a layer of additional controls which the citizen can employ in particular situations. The NDII should provide an adequate standard level of safety and security to meet the needs of most citizens in most situations. The citizen should not have to rely upon exercising Citizen Control in order to be safe.

A large part of Citizen Control is Citizen Consent. Citizen Consent allows the identity subject direct control over whether relying parties can access their NDII data or make particular uses of their data. It is exercisable in situations where it does not conflict with the legitimate interests of another participant in the NDII, which means primarily where it does not conflict with the public or national interest.

Another part of Citizen Control is Citizen Education. In order to exercise consent meaningfully, the citizen will need to be given a sufficient understanding of the main issues which have a direct bearing on their provision of consent. This revolves primarily around having a sufficient grasp of the risks and of the safeguards which are there for their protection.

A third part of Citizen Control is Informed Citizens. The citizen needs to have up-to-date knowledge about how well the NDII is working, so they know what sorts of things do go wrong from time to time and how likely it is their participation with the NDII will put them in harm's way.

Citizen Control is itself one part of the wider governance framework for the NDII. The UK Government should provide a comprehensive and independent assurance regime so the citizen can rely upon the correct and effective working of all the governance arrangements.

A summarised version of this report is available as IAAC Briefing Paper 68.

Background

Whilst remaining neutral with regard to the current UK Government's plans, IAAC recognises that the UK is likely to develop a national digital identity infrastructure (NDII) in one form or another in the coming years. IAAC's objective is to help ensure that the resultant NDII is reliable, safe and secure, and contributes positively to the UK's digital future.

IAAC's past research into Identity Assurance within the context of an NDII has shown that:

1. People will not willingly accept the idea of the UK having an NDII and agree to participate with it unless they feel it can be made sufficiently safe. (Even if participation is made mandatory for UK citizens, it is not expected that the government of a civil society would want to put itself in a position where it is seen to be coercing people to do something they felt was threatened to them.)
2. This is not to say that the NDII needs to be risk free, any more than the roads people drive on every day need to be risk free. However, it does mean that the NDII should be sufficiently and acceptably safe. For most people, it should be extremely unlikely they would be involved in a serious NDII incident or accident at any stage in their lifetime.

3. IAAC has shown that it is most important that the NDII should have safety nets in place to protect the citizen when things do go wrong. A major contributor to people's feelings of being safe with a new system is the presence of safety nets, i.e. recovery and restitution arrangements to deal with any damage or harm caused when things go wrong, for example, when a person's identity record gets compromised or corrupted.

4. However, UK citizens appear to be rather sceptical. They have doubts that the UK Government:
   - understands the dangers, i.e. how citizens could be harmed by an NDII;
   - can actually be a force for their protection;
   - has the competence to design and operate an NDII reliably, safely and securely.

5. Given these doubts, if the citizen is to feel sufficiently comfortable engaging with the NDII, the citizen will have to have the ability to make sure they can stay safe. Until people feel they can rely on the inherent safety of the NDII, they will want to have the ability to take any additional precautions they might feel are needed to keep themselves safe. This is what is meant by the term "Citizen Control". It is the citizen as identity subject having the ability to take particular additional precautions, when necessary, to ensure they stay out of harms way.

6. Citizen Control does not stand in isolation. The interests of the citizen are not the only interests being catered for by an NDII. The interests of the public (the public interest) also need to be protected, and there may be times when the legitimate public interest conflicts with the legitimate interests of the individual identity subject. Citizen Control needs to be embedded within a Digital Identity Governance Framework (DIGF) which protects the interests of all participants in proper balance, and which ensures that when the legitimate interests of the identity subject are overridden in the public interest, the citizen remains protected so their interests are not harmed unnecessarily or inappropriately in the process.

The subject of this March 2008 IAAC workshop was Citizen Control, i.e. what are the components which make up Citizen Control for a UK NDII. IAAC also ran a related workshop in April 2008 (reported upon separately) to look at an NDII DIGF, i.e. what are the components of a Digital Identity Governance Framework for a UK NDII.

Workshop Results

Key Messages

The key messages which emerged from the 5th March 2008 workshop are:

- The UK NDII should provide adequate safeguards to maintain an acceptable standard of safety and security for participating citizens. It should provide Citizen Control but it should not require people to exercise those powers in order to be safe.
- It is acknowledged that some people today do take unnecessary risks with their private data. It is also acknowledged that there has not been a general public outcry against the widespread use of CCTV in the UK. This does not mean that UK citizens are unconcerned about their privacy and is not an indication that there is no need for effective Citizen Control within the NDII.
- Citizen Consent should be free, fair and granular. It should at the same time be easy for the citizen to give enduring or acquiescent consent, or to delegate the power of consent, so they are not burdened with requests to exercise powers they do not understand or wish to exercise.
- If Citizen Consent is to be exercised meaningfully, the citizen needs to have a sufficient understanding of the issues that affect their provision or withholding of consent. For most people, this doesn't mean they will need to understand the risks in any detail, or that they will need to be familiar with the safeguards in any detail.

- Transparency is key. Transparency allows people to have confidence that they will be able to sort out any problems which might arise later, as and when those problems arise. Transparency allows people to tolerate risk more easily and not need to have all the risk and safeguard details be spelled out to them beforehand.
- Effective recoverability and restitution in the event of NDII failures and breaches is an essential component not only of the citizen's feelings of safety but also of making Citizen Consent meaningful. The provision of effective safety nets remains an important issue still to be resolved.

Findings

The following are the findings which emerged from the 5th March 2008 workshop[1].

Providing Citizen Safety and Security

People feel they have already lost a degree of control over their personal data. They don't know reliably who holds which personal information relating to them, and they don't have the ability to recall that data in order to reduce their exposure. Hence, people live with the risk that one day something might go wrong as a result of the exposure of their data, just as they live with the risk that one day they could have a nasty accident through their use of the roads.

The job of making the NDII sufficiently safe for the citizens who are its identity subjects is not a technological problem, it is a governance problem. Technologies can be developed and used to build whatever solutions, protections, safeguards and controls are desired. The effort needs to be put in to the digital identity governance framework (DIGF) to specify the protections, safeguards and controls that are desired so that the NDII can be made sufficiently safe. Only once that framework has been defined should the NDII Authority (the body or bodies which have authority to decide the NDII's development programme, its design and its operation) select a suitable architecture and technologies with which to deliver an NDII which meets the agreed specification.

The NDII DIGF will lay out the arrangements in place for the protection of the interests of NDII participants. There are a number of components to the DIGF, one of which is Citizen Control. The particular contents and details of the Citizen Control component are described in this report. The particular contents and details of the other components of the DIGF were discussed in the April 08 IAAC workshop and are reported upon separately (see IAAC Briefing Paper 69 and its associated full report).

The Purpose of Citizen Control

Citizen safety needs to be placed at the centre of the NDII's digital identity governance framework. This is not just a platitude to placate the wary citizen, this is a necessary step if the citizen is to feel sufficiently safe they can agree willingly to engage with the NDII.

Citizen Control serves to allow the citizen as identity subject to take particular additional precautions, should they feel that necessary, to protect themselves from harm in particular situations where they feel they are facing risks they would rather avoid.

Citizens should not have to rely upon exercising Citizen Control in order for them to be safe. The NDII should provide adequate safeguards to maintain an acceptable standard of safety and security for participating citizens in all situations where there is no conflict between the legitimate interests of the citizen and the interests of other NDII participants. The NDII should provide Citizen Control but should not require people to exercise that control in order for them to be safe.

Different citizens will have differing views of the sufficiency of that standard of safety and security, and some will want to have the ability to take additional precautions in situations where they feel themselves exposed to

[1] IAAC ran two workshops in the Spring of 2008, this March workshop looking at Citizen Control and an April workshop looking at the wider governance framework. Inevitably, some of the ideas which were raised in the discussion on governance related to Citizen Control. Where that is the case, the ideas have been covered in this report rather than in the governance framework report.

unnecessary or unwarranted risks. Citizen Control is the fine tuning that allows a citizen to reduce their risk in those particular situations, and is exercisable when its exercise does not conflict with an overriding interest of another participant (e.g. the public interest).

Various informal surveys have shown how readily people sometimes are prepared to give away private information "for a free supermarket chicken or a bar of chocolate". This can be taken two ways. It can be, and often is, taken to mean we need a better educated public. Alternatively, it can be taken as an indication of how people naturally behave in the absence of visible risks. It is human nature that some people will needlessly take unnecessary risks when the risk is not immediately apparent to them. As well as this behaviour being shown through the abovementioned informal surveys, it has been shown in other walks of life, for example in the way some people drive their cars. The NDII should provide adequate safeguards and, in addition, Citizen Control, but it should not presume that everyone will understand the risks, or that they will act to minimise unnecessary risks. That some people currently take unnecessary risks with their private data is not an indication that there is no need for effective Citizen Control.

It is often commented that there has been no significant public outcry in the UK against the widespread use of CCTV despite the fact that most people know that their movements get caught on CCTV possibly many times a day. It is similarly commented that in other cultures the expected outcry would likely have been sufficient to prevent such widespread use of CCTV elsewhere. This suggests that within a multi-cultural society, such as the UK's, even if there is not a general public outcry against the NDII, some citizens will still, legitimately, harbour significant concerns and discomfort. Citizen Control must allow people from all perspectives to feel that the existence of the NDII and the purposes for which it is used can still be made sufficiently safe it does not put them unacceptably at risk.

Citizen Control

A large part of Citizen Control is Citizen Consent, the ability of the identity subject to limit some aspects of their participation in the NDII and thereby minimise those situations which they feel present them with a level of risk they would rather avoid. There is, though, more to Citizen Control than just Citizen Consent. In order for Citizen Consent to be exercised meaningfully, the citizen needs to understand the issues that affect their provision or withholding of consent, and they need to be given up-to-date information regarding the operation of the NDII so they can base each consent decision on current information about how well the NDII is working. Each of these three components of Citizen Control will be described in this report.

Throughout the discussion of Citizen Control, it is important to bear in mind the practicalities of providing these powers. To be effective, Citizen Consent powers need to be easy for the citizen to understand, to take on and to apply. The granularity of Citizen Control needs to be adjustable on a citizen-by-citizen basis so those who wish to exercise close control can do so whilst those who are satisfied with a much lower level of direct control are not burdened with controls they do not understand or wish to exercise.

Citizen Consent

The first part of Citizen Control is Citizen Consent. Citizen Consent is the ability of the citizen as identity subject to mitigate their risks in situations where they feel that is needed. Within the context of the NDII, the risk to the identity subject arises from the possibility that others, i.e. relying parties, might use the subject's personal information in a way which harms the subject's personal interests. Hence, Citizen Consent is about the citizen being able to deny relying parties the right to use their information in such ways.

Citizen Consent should allow the citizen:

- To restrict what information is provided to a relying party (for example, in the context of a private sector service provider, to withhold address details if those are not needed for the provision of the service);
- To restrict the purposes for which provided data may be used (for example, in the context of a private sector service provider, to permit the data to be used to provide the requested services but not for marketing other services or developing sales materials);

- Within the context of an approved purpose, to constrain the way in which the provided data may be used (for example, in the context of a public sector service provider, to allow the data to be used to verify entitlement but not to be used for profiling the individual taking the service).

The range of purposes and actions which are permitted for relying parties will be defined in the NDII governance framework. The citizen should not be asked to provide consent except for permitted purposes and actions. They should not be asked to provide consent for trivial matters or for matters which do not relate to their interests, and should not be asked to provide consent outside the times when their consent is to be applied.

The citizen should have the option to provide enduring consent, to be acquiescent (forego the right to have their consent be sought) and to delegate their power of consent to another (e.g. an agent or proxy) should they so wish. Provided the NDII proves itself to be sufficiently safe, citizens should at some stage (some sooner than others) develop trust in the way the NDII and its systems work, and can then relax their reliance on having direct control over their granting of consent. Relaxation of direct control requires trust which in turn requires the NDII to demonstrate that it is safe and its safeguards are effective. Where the citizen has relaxed their direct control over the exercising of consent (including where they have provided enduring or acquiescent consent), they will need to have the ability to reassert their direct control and revoke those arrangements at a later date should they so choose.

The citizen's choice of whether or not to provide consent needs to be real (informed and free) and not coerced. If it is real, the user will believe they have meaningful control and as a consequence will feel that their participation with the NDII can be safe. If not real, or if they feel coerced, they will not feel they have meaningful control and as a result will not feel sure that their participation can be made safe.

The citizen's choice needs to be fair. Any reduction in the service or benefit the citizen receives needs to be directly and reasonably a result of their withholding or restricting consent, and no more. This requires that there should be an adequate level of granularity in the choices put in front of the citizen. Standard privacy policy statements as provided to users on the web today are often not sufficiently granular and, as a result, are often not particularly fair. They do not, typically, provide the user with options other than to accept or decline the policy as a whole, and declining the policy as a whole usually means that the user does not obtain the goods or benefits they were seeking. The citizen should have the ability to withhold consent to specific aspects of the proposed actions which they feel they would rather not accept, and the ramifications in terms of any reduction or loss of service or benefit must be no more than that which is a direct and reasonable result of their decision. Relying parties should not be allowed to exploit the citizen's need or desire for a service or benefit to gain unnecessary consent to access, use or retain a citizen's private data.

There may be some situations where there is a tension between two citizen safeguards. For example, one important safeguard is the auditability of what data has been provided to which relying party and how that data has been used by that relying party. However, the more comprehensive and detailed the auditability provided within the NDII, the more the individual's privacy can be invaded. Increasing privacy safeguards within the NDII so its operators cannot see all the uses the citizen has made of their NDII data can lead to a loss of auditability. To the extent that the design of the NDII is not able to resolve such tensions and allow both conflicting safeguards to be satisfied in full, Citizen Consent should, within limits, enable the citizen to adjust the balance between the two safeguards to minimise their perception of the overall risk.

The processes by which the citizen is asked and provides consent need to be broadly consistent across the various different invocations and contexts. This would help the citizen to develop an understanding of the dynamics of Citizen Consent and would ease their management and control of their provision of consent.

Citizen Education

The second part of Citizen Control is Citizen Education. If Citizen Consent is to be exercised meaningfully, the citizen needs to have a sufficient understanding of the issues that affect their provision or withholding of consent.

People understand the risks of using the roads, not in the sense of being able to quote the probabilities of this or that type of accident occurring, but in terms of knowing the range of possible outcomes (from scratched

bodywork through to motorway pile-up) and the range of possible harms (from light bruising through to major physical trauma and even death). People do not yet understand the risks they face from the NDII, i.e. in what ways it might matter to them if the NDII holds, or other parties have access to, identifying information relating to them. The UK Government should aim to get citizens to a similar level of broad understanding of NDII risk-relevant issues to that people have for their use of the roads. It probably does not need to get more than a small minority of citizens to a more detailed level of understanding of the risks.

Similarly, without their knowing any specific detail, most people appear generally to have faith that there are protections in place on how CCTV surveillance is used, protections which ensure that they as individuals are highly unlikely to be affected adversely by the improper use of CCTV. This suggests that if UK Government can give the citizen a similar degree of confidence that there are plenty of safeguards in place to ensure they are protected (i.e., highly unlikely to be affected adversely by the improper use of NDII data), most people will not need to know the particular details of what those safeguards might be.

Risk tolerance increases with transparency. If people have confidence all the information they might need is available to them somewhere, they tend to feel more risk tolerant. Transparency allows people to have confidence that they will be able to sort out any problems which might arise later, as and when those problems arise, and not need to have all the risk and safeguard details be spelled out to them beforehand.

Notwithstanding the above points, people will still need to be helped to understand the purpose of Citizen Control and the powers it provides. This is not only so they can exercise those powers properly when they need to but also so they do not take Citizen Control to mean something which it is not or to provide powers which it does not. Either the UK Government or the NDII Authority needs to provide a communication piece that explains the purpose of Citizen Control and how the citizen might expect to exercise those powers.

The identity subject will need to be given a way to find out what information relating to them is held within the NDII. The citizen should also be able to find out the rate at which their data has been accessed by which types of relying party so they can, if they wish, how much their data is known or held by parties out in the field.

Where there are particular trade-offs or balances to be applied between safeguards, such as between auditability and privacy, the NDII Authority will need to provide a communication piece that explains the conflict and the arguments on either side of the trade-off so the citizen can exercise their consent accordingly.

Informed Citizens

The third part of Citizen Control is keeping the citizen informed. In order to exercise Citizen Consent, the citizen needs to be given up-to-date information regarding the state of operation of the NDII. This is so they can base each consent decision on current information about how much their participation with the NDII is likely to put them in harm's way.

Citizens will need access to public information, provided either directly from the NDII Authority or through the media. This information should cover, at a minimum:

- The level of use of the NDII. How often are NDII records accessed, hardly ever or constantly? And by what types of relying party and for what purposes? The more heavily the NDII is used, the more the citizen is exposed to risk, and the more likely the citizen is to want to exercise Citizen Consent powers to reduce their risk in those situations they perceive to be the riskiest.
- What failures, errors, misuses and abuses are taking place, and how often the different types of problem arise. People expect the custodians of their data (NDII operators and relying parties) to take good care of that data. The UK Government needs to ensure the public is informed whenever significant failures or breaches occur.
- Descriptions to show that the safety nets in place to protect the citizen when things go wrong are working. For both large and small failures, reports should describe what the outcomes of those failures are (how many people got hurt and in what ways) and how people have recovered from the damage they have sustained and the harm they have been caused.

The issues of recoverability and restitution in the event of failures and breaches have still to be addressed for the NDII. Throughout its research into NDII identity assurance issues, IAAC has been reporting that recovery and restitution issues have a large part to play in the degree of confidence the citizen feels with respect to the safety and security of the NDII. Effective recoverability and restitution is also an essential component of making Citizen Consent meaningful. If the citizen cannot see how a problem would be resolved if something were to go wrong, for example if they cannot see how their identity would be repaired if compromised, or how any erroneous loss of rights or entitlement would be made good, they might well feel that no amount of Citizen Consent can make up for the risks they are being asked to face. The provision of effective safety nets remains an important issue still to be resolved. For more on this issue, please see IAAC Briefing Paper 69 and its associated full report on IAAC's April 2008 workshop.

The citizen will also need means to obtain confirmation that the protections and safeguards on which they rely are operating correctly. The UK Government should put in place an assurance regime which checks, independently, in full and on a regular basis, that all aspects of the NDII DIGF are covered by suitable arrangements which are in place, operational and effective. As it is relying parties and their applications which make use of NDII data, the assurance regime will need to cover all relying parties and their applications as well as the core NDII. In addition to reporting regularly to a suitable body (e.g. Parliament), the NDII Commissioner at the head of this assurance regime should put assurance reports appropriate for general consumption into the public domain.