

Data sharing and data protection

National Consumer Council's response to the Data Sharing Review
February 2008

1 Introduction

The National Consumer Council (NCC) welcomes the opportunity to respond to this consultation.

NCC represents the interests of consumers, which we define to include “everyone in society in one part of their life: that is, as the purchaser or user of goods and services, whether privately or publicly supplied.” NCC’s mission is to help everyone get a better deal by making the consumer voice heard. Our strategic objectives include those of placing users at the heart of public services and ensuring that disadvantaged and vulnerable consumers get a fair deal.

Overall, we are concerned that the consultation over-emphasizes data sharing over data protection. We make a number of recommendations on improving data protection and respond to selected questions in the consultation. We believe that the data protection regime needs to be improved in the UK:

- Notify individuals when their personal data is leaked
- Increase penalties for failing to protect personal data
- Improve redress for consumers who have had their personal information released to unauthorized users or for unauthorized uses
- Increase the authority of the Information Commissioner’s Office to investigate and prosecute violations and ensure adequate funding for the office
- Mandate standards to address poor security management in organisations
- Require independent privacy impact assessments before allowing new collections or uses of personal information
- Ensure consumers have clarity on the uses of their personal information, including information sharing
- Encourage development and use of Privacy Enhancing Technologies
- Promote consumer education on privacy and data protection through effective and targeted social marketing campaigns

2 General issues

2.1 NCC and privacy

Over the past 10 years, the NCC has been actively involved in policy issues relating to personal information including participation in the Cabinet Office’s Performance and Innovation Unit’s review in 2002 and the publication in 2004 of the study *The Glass Consumer* setting out a new agenda for protecting privacy in the information age.

It is well recognized in domestic and international law that privacy is a fundamental human right essential to protecting individuals as both citizens and consumers. Of prime concern to individuals is the loss of control and intrusion into their personal lives resulting from a lack of privacy. Other concerns include the mishandling of information that can lead to identity theft, and the dissemination of inaccurate information that can result in social stigma or loss of credit or benefits.. There are also concerns over digital redlining and information exclusion, where consumers are adversely affected by the use of personal information, to favor some persons over others.

Protecting privacy is also crucial for those bodies that wish to use personal information in their operations. Without adequate protections, both public and private sector plans to use personal information, including e-government and e-commerce, can be undermined by lack of public trust and consumer confidence.

This should already be a concern for officials. The annual polling from the Information Commissioner's Office shows that there is strong public concern about protection of its personal information. In 2007, 94 percent of individuals listed "Passing or selling your personal details onto other organisations" as a major concern.¹ 94 percent also listed "not collecting and keeping your personal details secure" as a concern. In a 2006 poll commissioned by the Joseph Rowntree Reform Trust, 56 percent opposed "Allowing government departments and public bodies to share personal information they hold about any person without consent."² The most recent poll from 2008 found that 52 percent were uncomfortable with proposals "To allow personal information that is provided to one government department to be shared between all government departments that provide public services".³

2.2 Government emphasis on data sharing

We must first state a preliminary concern that the review seems to be slanted towards encouragement of sharing data rather than a much more needed comprehensive review of the adequacy of the Data Protection Act 1998 and its implementation.

It is our view that the sharing of data does bring benefits to consumers in some circumstances.. Examples of such circumstances include timely passing of data to relevant bodies when a person dies, to prevent deceased identity fraud; ensuring that services reach disadvantaged members of society, while limiting excessive repetitive requests for information to such groups; and protection of vulnerable children.. However, we believe that any data sharing must be done based on the consent of the individual within the framework of a strong and enforced data protection system. Unfortunately, that does not currently exist in the UK.

Over the past decade, it has appeared that government policy has been preoccupied with data sharing while paying little attention to data protection, except as a barrier to be minimized or overcome. Following the 2002 Performance and Innovation Unit (PIU) *Privacy and Data Sharing* report and consultation, there was also the Lord Chancellor's Department *For your information* consultation in 2003, the 2005 *Transformational Government* consultation, and the 2006 *Information sharing vision* statement. The Ministerial Committee on Data Sharing (MISC31) was also created to "to develop the Government's strategy on data-sharing across the public sector". In all of these, proposals on increasing data sharing were made.

The consequence of these policies has been the increase in the last few years of large-scale information systems, sharing personal information where privacy and data protection concerns seem to be ignored. These include the National Identity Register, Contact Point and NHS Spine. We urge further investigation into whether these systems, which will hold sensitive information, have adequate protections against unauthorized access. As we have noted before, the creation of a centralized single system of personal information, which is shared between bodies, is "not necessary or desirable".⁴ Information that is not relevant to specific services should not be shared between departments.

Meanwhile, little has been done to evaluate the effectiveness of the Data Protection Act. Many of the consultations and statements suggested that privacy is important and proposed improving privacy protections as part of data sharing. The PIU report made a number of useful suggestions to improve the internal management of public

¹ Annual Track Results 2007, 7.2.4.

² JRRT, State of the Nation 2006

³ JRRT, Public Data Security Survey, CATI Fieldwork : February 1st-3rd 2008.

(<http://www.jrрт.org.uk/ICM%20Omnibus%20poll%20-%203%20February%202008.pdf>)

⁴ NCC, Government Direct: a Prospectus for the Electronic Delivery of Government Services, January 1997.

bodies in how they handle personal information but the recent series of data breaches would indicate that few, if any, of those recommendations were adopted in practice. Similarly, public awareness of data protection rights and how personal information is used remains very limited.

Of particular importance are the reports that the European Commission has found the UK not in compliance with the EU Data Protection Directive in many areas and is currently considering an enforcement action against the UK to improve the Act and its implementation.⁵ To date, the UK Government has refused to release any details about the EU concerns with the Act. Given the importance of privacy as a basic human right, we urge the Government to make public the concerns and its' plans for addressing them.

⁵ According to a letter from the EU Commission, these are “Articles 2, 3, 8, 10, 11, 12, 13, 22, 23, 25, and 28 of the Data Protection Directive (95/46/EC).” Email to journalist Chris Pounder from Francis Svilans, EC official, 13 September 2007.

3.Improving current laws and practices

3.1 Data breaches and security

Adequate security is a vital principle for the protection of personal information. The large number and scale of recent data breaches of personal information, many coming in the process of data sharing, indicate serious problems with implementing the rules on the holding and processing of personal information.

The scope of the problems, ranging from lost disks and computers, to sensitive files placed in publicly accessible rubbish bins, to insider abuses, to weak security on government web sites indicates a widespread cultural problem rather than a specific area of weakness. A poll by YouGov released in November 2007 reports that 1 million employees in the UK have lost disks, drives or laptop computers, which contained confidential personal information.⁶

We note that the government itself recognizes problems with security and offers higher security measures for certain officials and celebrities.⁷ We believe that the personal information of all persons should be protected, not just a select few.

To improve data security, we believe the following measures should be adopted:

- *Notification.* Individuals should be informed immediately when their sensitive personal or financial information is accidentally or deliberately disclosed to unauthorized parties or lost.
- *Mandatory Security Requirements.* There should be specific binding requirements on data security of personal information to ensure that the current outbreak of breaches does not continue. This should include the use of encryption, audit trails, increased access controls, and regular security audits.
- *Credit Record Freezes.* As a means to limit identity theft, there should be a free and easy-to-arrange mechanism to “freeze” personal credit records to ensure that consumers have control over their financial information and are not subject to fraudulent lines of credit. This model, or one of opting out, may also be appropriate for other large systems of information.
- *Remedies.* We also believe that individuals should have adequate remedies when their personal information is disclosed deliberately or negligently. Individuals should have the right to obtain damages for the unauthorized disclosure of their personal information without having to show specific harm such as for distress. This could be in the form of statutory damages as are set up in the USA under the Privacy Act of 1974. The mechanism for enforcing this should be easier than filing a lawsuit and should allow for collective redress.
- *Increased access.* Fees for subject access requests should be waived for information in electronic systems. Individuals should also have access to all personally identifiable information that is shared, and with whom it is shared.

⁶ One million UK employees admit to losing confidential data, PersonnelToday.com, 21 November 2007.

⁷ Online tax system 'too risky' for the famous, Daily Telegraph, 28 January 2008.

3.2 Oversight role of Information Commissioner

The Information Commissioner's Office (ICO) plays a critical role in ensuring that individuals' privacy rights are protected. However, the ICO is limited in a number of crucial ways that undermine its ability to operate effectively.

A major area of concern is the lack of the powers for the Commissioner to enforce the Act. The Commissioner appears to have fewer abilities than his counterparts in other EU countries to investigate and enforce the law. This is not a new concern. Many of the commentators to the 2000 consultation recommended changes but none were adopted.⁸

NCC believes that the following measures should be adopted to improve the effectiveness of the ICO in protecting personal data:

- *Stronger powers to investigate.* Currently, the ICO cannot conduct audits of data controllers without the permission of the controller. We welcome the recent government announcement following the HMRC and DVLA data breaches that the ICO will now be given the power to audit government departments without prior permission. However, we believe that this power should also extend to private sector bodies where there is sufficient evidence that substantial violations of the act are occurring. This power is common in other European countries and is likely to be one of the areas where the European Commission will require changes with existing practice.
- *Increased powers to improve compliance.* The ICO should have additional powers to obtain quick and effective injunctive relief, extended information notices, requiring skilled assistance and naming and shaming.
- *Review and approval of new data sharing schemes.* The ICO should be required to review and give approval of new data sharing schemes prior to their adoption. The system could be funded by requiring government departments to pay fees to the ICO for the review of the proposed schemes.
- *Adequate funding.* It is well recognized that the Information Commissioner's Office is not adequately funded to conduct effectively his jobs for both the Data Protection Act and the Freedom of Information Act. While the budget of the ICO is between £10 million and £15 million each year, other bodies with similar regulatory tasks are far larger. The new Equalities and Human Rights Commission's budget is around £70 million, the Office of Fair Trading's is nearly £80 million and Ofcom's budget is over £120 million. This low budget has had severe consequences: public information and awareness campaigns are inadequate; proactive investigations have been set aside; and staffing is quite low compared to the tasks, so delays are rife. This has hampered enforcement of both the Data Protection Act and the Freedom of Information Act.
- *Combining Oversight Bodies.* Oversight for protection of privacy in the UK has been segmented into a number of different bodies. The Information Commissioner oversees data protection while the Surveillance and Interception of Communication Commissioners oversee issues relating to access to telecommunications data and wiretapping and the new Identity

⁸ "Most respondents who commented on this question felt that the Commissioner should have stronger powers (and more resources). A number of the specific suggestions related to her powers to conduct assessments." DCA, Data Protection Act 1998: Post-Implementation Appraisal Summary of Responses to September 2000 Consultation, December 2001

Commissioner will oversee issues under the Identity Cards Act. Given the strong overlap of these issues, especially relating to Data Protection and the National Identity Register, it makes little sense to have different Commissioners with different powers. We suggest that the offices be combined under the ICO with appropriate funding made available. This would also remove concerns that some authorities are not sufficiently independent of the bodies that they are supposed to be overseeing.

3.3 Increased penalties for violations

Currently the penalties for violations of the Data Protection Act (DPA) are extremely weak, and rarely invoked, which encourages non-compliance. We welcome current proposals to increase the penalties for violations of the DPA.

Civil fines under the DPA are lower than the cost of doing business. We believe that a scheme of strong civil penalties should be available similar to those used by the Financial Services Authority in the case of the data breaches at Nationwide and Norwich Union. These penalties are available to privacy regulators in other jurisdictions such as in Spain and Greece.

We also agree that in some circumstances criminal penalties should be imposed for deliberate or grossly negligent violations of the DPA. Currently, criminal penalties are nearly non-existent. Police often use other laws such as those on fraud rather than DPA to increase the penalties. At the same time, Section 59 of the DPA imposes stronger criminal penalties on the ICO for releasing information than on those who violate the substantive provisions of the DPA.

We also believe that administrative sanctions should be available against government bodies that fail to follow the requirements of the DPA.

In addition, as noted above, we believe that consumers should have the right to substantive damages for the unauthorized disclosure of their personal information such as for distress and lost time without having to show specific harm. This should include the ability to obtain collective redress.

4 Response to consultation questions

4.1 Private sector holding too much information (Q6)

As we have noted in previous consultation responses, the collection of personal information has become increasingly sophisticated in the past decade. More and more information is collected about consumers. This is of particular concern with Internet-related communications.

Currently, search engines such as AOL and Google and advertising networks such as DoubleClick collect significant amounts of personal information about users, much of which is personally identifiable. These companies retain the information for long periods of time and use it to develop complex profiles about users for marketing purposes. Many also make it difficult for users to delete their accounts and information once it is in their systems.

We are especially concerned with recent efforts to merge a number of these companies including Google and DoubleClick and Microsoft and Yahoo. Besides the obvious competition issues for consumers with the vast majority of searches and advertising being controlled by only two companies, there are serious privacy

concerns about the vast amount of data that is being held by these companies and the potential for merging databases, consumer targeting and personal privacy invasion.

We are also concerned about the collection of information about children by web sites and its use for marketing. In our recent report *Fair Game*, we found that data protection rules were often ignored, hidden persuasion techniques were used and different jurisdictions' age rules confused parents and children.⁹ We made a number of recommendations to the ICO, the Advertising Standards Agency and the industry to improve data protection practices including examine ways of improving communications to children on DPA issues, pursue adoption of plain English privacy notices, and better enforce the law, including through international co-operation.

4.2 Improper sharing of data (Q8)

Currently, there is little publicly available information on the sharing of information by the public or private sector. The few examples that we are aware of raise grave concerns about the potential for misuse.

- *NAO*. The recent revelations about the loss of data between NAO and the HMRC are an interesting case in point. It has been reported that the NAO request for less information was rejected because of concerns that the private contractor would charge for revising and limiting the amount of data sent. This raises questions about both data protection and the outsourcing of personal information to private sector bodies that are given a de facto ability to control access.
- *Insider abuses*. In recent years, there have been dozens of cases where public officials, including employees from the police, DVLA and HMRC have been arrested for unlawfully disclosing personal information for financial or personal reasons. The large-scale databases that are currently being created will likely increase this problem.
- *Access to private telecommunications data such as calling records and home addresses*. The Surveillance Commissioner revealed in his most recent report that 1,000 records a day are being accessed by nearly 400 public bodies with very little oversight. This wide scope of the collection and access of information is highly concerning. We note that in previous years, the Commissioner has complained about not having enough staff to do an adequate job of oversight while thousands of problems are found each year under the scheme. Little has been done to improve the adequacy of the procedures.
- *DVLA*. We also are concerned about the system of access to the Driver and Vehicle Licensing Agency's vehicle register. The system of allowing access to anyone with 'reasonable cause' seems to have a very low threshold and there have been reports that records are legally passed onto convicted criminals. Over 5 million records in the past five years have been disclosed. We welcome the ICO's recent guidelines but believe that further investigation into access limits should be conducted.

⁹ NCC, *Fair Game: Assessing commercial activity on children's favourite websites and online environments*, December 2007.

4.3 The Effectiveness of the DPA (Q9)

As noted above, we have significant concerns about the effectiveness of the DPA as written and its implementation. As we have said before, the DPA is “a lengthy and often ambiguous piece of legislation that many find hard to understand.”¹⁰

In *The Glass Consumer*, we called for simplification of the law while ensuring that core protections are retained in a more effective manner. As part of that, NCC made a number of recommendations on improving the Data Protection Act. These include:

- Clarify the definitions of consent, relevant filing systems, legitimate interests and personal information following the *Durant* decision.
- Limit collection of true identities including identification numbers to those cases when absolutely necessary.
- Give regulators the power to control use of data matching algorithms to help limit incorrect assumptions.
- Consumers should also have more detailed access to information on who their personal information is being shared with.

As we noted above, we also have serious concerns with the powers of the ICO to investigate and enforce the act. NCC also believes that consumers should be given more powers to enforce their rights and in obtaining damages for harms to privacy that arise from a failure to follow the law.

We also wish to emphasize strong opposition to previous government proposals to amend the DPA to create new frame works to allow sharing using secondary legislation or create “opt-out” systems to facilitate data sharing.

4.4 Consent (Q16)

We believe that the use of personal information, especially for purposes not originally intended when it is collected should be based on informed consent. A number of principles are important:

- *Consent is informed.* Individuals must be given full information on the reasons for the collection of information, who will have access to it, and what it will be used for. They must also be informed about their rights for access and control.
- *Consent is given explicitly.* A fundamental principle of consumer law is that consent is explicit. We are concerned that some bodies are now considering consent to be implied, even in the cases of sensitive information such as medical records. We believe that this is not proper and may not be legal.
- *Consent is voluntary.* We oppose any schemes where the denial of consent to data sharing leads to detriment for the individual, especially the denial of critical services such as health care or other types of essential assistance.

As we noted in the *Glass Consumer*, there are concerns about the lack of an agreed definition of consent, especially implicit consent in the DPA. We recommend that definition be clarified to ensure that individuals are aware of the sharing and give an affirmative agreement to it.

¹⁰ The Glass Consumer, p 227.

4.5 Transparency of data sharing (Q18)

NCC has long believed that in consumer affairs transparency is a crucial principle. There appears to be little public awareness of the actual scope and scale of data sharing by government bodies. It is crucial for fostering an informed discussion on data protection and data sharing that better information about practices is made public.

There appears to be a regrettable lack of information around many of the major ICT proposals that involve data sharing, especially relating to the creation of the National Identity Register and the NHS systems. Many requests under the Freedom of Information Act have been rejected on grounds of confidentiality. It is crucial that information is available for an informed debate while the systems are being developed as once they are in place, it will be difficult to make changes.

Even when there is information available, it is often difficult for consumers to understand. As noted above in our comments on consent, there needs to be better notice given to people who provide their information. The notices need to be written in plain English so that they are understandable, but also give enough detail so that individuals can fully understand what is being done with their personal information and what their rights are relating to the data and those uses.

Access by individuals to their own personal information and its uses should be facilitated. People who use the subject access request provisions of the Data Protection Act should be automatically informed of all uses of their personal information. The uses of electronic systems to allow individuals to access their own personal information should be continued with adequate authentication mechanisms.

One proposal mentioned in the PIU report that all data sharing schemes should be detailed in publication schemes under the Freedom of Information Act should be immediately adopted. There should also be a regular compilation of Central Government sharing such as required in the US under the Computer Matching and Privacy Protection Act.

4.6 Framework codes and privacy impact assessments (Q19)

Framework Codes

Framework codes such as issued by the Commissioner can be useful instruments for providing better clarity on the legality of data sharing. However we are concerned that they not be used in absence of clear legal authority allowing for the sharing.

More significantly, there is a problem with relying on Codes of Practice in the absence of real enforcement of data protection principles. The 2006 *Information sharing vision statement* highlighted the Code of Data Matching Practice 2006 applying to the National Fraud Initiative as a model for protecting privacy while facilitating data matching. Yet it was as a result of data sharing under the NFI that the nation's most serious breach – the loss of 25 million records sent from the HMRC to the National Audit Office – occurred. It remains to be seen what were the specific failures that led to that disclosure. But is clear that many of the DPA and Code's provisions on minimization of data and security were not followed.

Privacy Impact Assessments

NCC has long advocated for the adoption of consumer impact assessments in the developments of new policies to ensure that the consumer perspective is included. Likewise, we believe that privacy impact assessments are an important aspect of evaluating any new proposals, which may impact on individuals' privacy or personal data.

We believe that privacy impact assessments should be mandatory at least for any public body that is considering creating new policies or modifying existing ones that could affect privacy or personal data.

However, a privacy impact assessment that is only developed internally by those in charge of implementing new proposals raises concerns about its independence and transparency. We believe that it would be better that privacy impact statements are done by outside independent entities.¹¹

The assessment should be conducted at the early stages of development and shared with interested parties including the Information Commissioner, Parliament and the public for consultation before going forward with the proposal. As we noted with consumer impact assessments, this would allow for better quality policies: "If problems emerged with the policy following an appraisal, the Government could amend the proposal to deal with them; gather more information about the effects of that proposal; or decide for other reasons they need not amend the policy."¹²

4.7 Technical security requirements (Q21)

It is apparent that the current requirements in Principle Seven of the Data Protection Act, which require "appropriate technical and organisational measures", have not been sufficient to prevent poor security management in many organisations and the significant loss of personal information.

We believe that the legal requirements should be enhanced, perhaps through secondary legislation, to include more detailed policy requirements such as audit trails on access of personal information, limited access schemes to ensure that only those with access to personal data have it, and limits on the taking of personal information outside of secure areas without data encryption. There should also be mandatory periodic audits of all information systems that hold personal information to ensure that the security measures are adequate.

4.8 Privacy Enhancing Technologies (PETs) (Q22)

Privacy Enhancing Technologies (PETs) can be an important means of reducing potential privacy problems by limiting the amount of personal information that is collected or disclosed.

While there has been considerable discussion over the years about PETs, their use in protecting privacy by government departments appears in practice to have been quite limited. In some cases, techniques to allow sharing of information without identification have been actively opposed by government bodies such as the Scottish

¹¹ See e.g. Enterprise Privacy Group, Department of Work & Pensions Information & Analysis Directorate, Preliminary Audit of IAD Systems, 11th January 2005.
<http://www.dwp.gov.uk/asd/longitudinal_study/EPG_final_Report.pdf>

¹² NCC, Modernizing Government: The Consumer Perspective, July 1999.

Common Services Agency.¹³ In other cases, technologies such as biometric readers for school children have been promoted as privacy enhancing, on unsecured systems and without parental consent.¹⁴

We would encourage further development and use of PETs and would like to see their uses legally mandated once technologies are more mature. However, we do not believe that they should be used at the expense of legally enforceable rules on the collection and use of personal information. We believe that the two should be adopted in conjunction.

- Ends -

¹³ Common Services Agency v. Scottish Information Commissioner [2006] ScotCS CSIH_58 (01 December 2006).

¹⁴ EDM 686, Biometric Data in Schools,
<http://edmi.parliament.uk/EDMi/EDMDetails.aspx?EDMID=32367&SESSION=885>