

# Data Sharing Review

Richard Thomas and Dr Mark Walport

## Consultation paper on the use and sharing of personal information in the public and private sector

### List of questions for response

We would welcome responses to the following questions set out in this consultation paper. Please follow the question order as set out in the consultation paper, leaving a blank response box for any questions not answered.

Please email your completed form to [contact@datasharingreview.gsi.gov.uk](mailto:contact@datasharingreview.gsi.gov.uk)

Alternatively you can send a hard copy response to:

**Data Sharing Review Secretariat**  
**5.26 Steel House**  
**11 Tothill Street**  
**London**  
**SW1H 9LJ**

Thank you.

### Section 1: Background

Question 1.

*Comments: Sharing police information (non-personal and personal information) is a fundamental activity in the prevention, reduction and detection of crime and protecting communities. The police service shares information on a daily basis within the service, with partner agencies and the public. Information sharing allows for effective decision making.*

*We collect personal information on victims, witnesses, suspects and offenders. We also process information relating to police incidents.*

*Police information is collected through a range of police activities, managed through business processes and technology enabled systems. The collecting and recording of police information is key to effective policing. Personal information is collected covertly (eg surveillance) and volunteered (eg a report of crime, report of a road traffic incident). Information volunteered by witnesses for one purpose may be used for a purpose they are unaware of when providing the detail (eg shared with insurance companies).*

*Personal information is collected, held and shared for a police purpose, ie:*

- Protecting life and property*
- Preserving order*
- Preventing the commission of offences*
- Bringing offenders to justice*
- Any duty or responsibility arising from common law or statute law*

*As an employer the police service collects personal information relating to staff - personnel records, misconduct records, occupational health records. This type of information is shared with other agencies and external companies for administrative purposes eg banking, IT access.*

## **Section 2: Scope of personal information sharing, including benefits, barriers and risks of data sharing and data protection**

### Question 2.

Comments: a) Individuals – Prevention and detection of crime, protection of vulnerable persons and enables effective investigation of offences. EG disclosure under Part V Police Act 1997 – Criminal Records Bureau scheme to ensure employers have sufficient information to make a judgement on the suitability of a potential employee when working with children or vulnerable adults. Sharing of information ensures that other records are updated and accurate.

b) Society – Safeguarding our communities, eg tackling anti-social behaviour, terrorism and domestic extremism; address problems caused by alcohol, drug and substance misuse.

- Meet statutory obligations to involve the community eg through Neighbourhood Watch and Victim Support schemes.

### Question 3.

Comments: a) The risk to individuals is that personal information may be inappropriately shared with an adverse outcome for the individual which is disproportionate to the purpose for which the information is shared. The police service seeks to eliminate such risk by ensuring that appropriate steps are taken on a case by case basis to ensure that the sharing is both necessary and proportionate. Additional information provided to the CRB for employment purposes has raised a number of concerns surrounding the relevance test which is applied by Chief Officers. This decision needs to balance our duty to protect children and vulnerable adults but at the same time give due consideration to the impact such disclosure would have on a individual's life and career.

To minimise the risk to individuals it is important to (1) monitor agreed practices and processes for sharing information; (2) ensure clear and robust Information Sharing Agreements are in place when information is shared outside of the police service. (3) educate staff on the legislative powers that can facilitate information sharing; (4) ensure all agencies update their partners on changes to personal details (eg completing all fields in a partial file, adding final outcome); (5) ensure agencies in receipt of police information understand their responsibilities.

b) If the police service fails in its obligation to protect the personal information the public will very quickly lose confidence and trust in our ability to undertake our responsibilities. The recent high profile cases relating to loss of personal data by other public sector organisations

clearly illustrates the obligations of the police service in this respect.

#### Question 4.

**Comments:** The greatest opportunities are that the police service can share generic crime and incident statistical data, and personal information, to enhance performance in achieving policing objectives. There is an opportunity for partner agencies to use “joined up” IT systems to share information, and to share policy, processes and security measures for the systems.

The greatest risk is a failure to effectively share information leading to injury or loss of life, e.g. The Soham murders, information sharing issues as identified within the Bichard Inquiry.

#### Question 5.

**Comments:** The police service is not in a position to comment on other public authorities in this respect. As regards the police service, the introduction of the Management of Police Information Code of Practice (MoPI) and associated guidance provides a number of key principles for the recording of police information, and ensures that personal information is managed in accordance with the data quality principles – accurate, adequate, relevant, timely.

Historically, the Police Service used to weed conviction information from the Police National Computer. ACPO recognised that this was inappropriate and introduced the Retention Guidelines for Nominal Records on PNC, incorporating a ‘step model’ which ensures that such information is kept for much longer retention periods and is appropriately shared with non-police organisations.

There is a view shared by some within the police service that too much data is held within the police service on ethnicity and gender of victims and witnesses to meet statistical requirements, as opposed to meeting the operational requirements of policing.

#### Question 6.

**Comments:** No examples identified

#### Question 7.

**Comments:** Sharing of police information within the service and with partner agencies, the public promoted as good practice in line with the MoPI guidance. Police forces actively seek opportunities to share non-personal information, and personal information is shared subject to safeguards. Information Sharing Agreements have been introduced under MoPI to ensure consistent and proportionate sharing.

The legislation can sometimes be perceived as complex and bureaucratic. The Bichard

Inquiry identified that legislation was a barrier to information sharing in that police officers and staff were nervous about breaching data protection legislation.

There are financial barriers to introducing computer aided technology, as highlighted by the need for a national information sharing data base in the police service (Bichard recommendation).

It is difficult to obtain information from the Health Service, despite the benefits of sharing such data in public protection matters. For example, in relation to the drug treatment of individuals, sharing information with agencies involved in Integrated Offender Management.

Improving the ability of the police service to share fingerprints and DNA with jurisdictions outside of UK would be beneficial for identification and elimination purpose, particularly given the increasing number of migrant communities within the UK.

#### Question 8.

Comments: Following an Information Tribunal in 2005, ACPO established a PNC Information Access Panel to review organisations which access information held on the PNC. This Panel continues to monitor organisations with access to PNC and where appropriate removes such access.

The ACPO Criminal Records Office is concerned that the control and custodianship of personal data held by the police will be removed from the police in the future, for example passing to a private organisation, with the potential that access and sharing arrangements would be governed more by economic considerations than operational requirements.

### **Section 3: The legal framework**

#### Question 9.

Comments: Data Protection has for any years been incorrectly viewed as a negative and over restrictive piece of legislation. The Code of Practice on the Management of Police Information and guidance set out principles to provide a common national framework for the police service, which will negate some of the uncertainties that individuals have when it comes to processing personal information.

The Data Protection Act, and in particular Schedule 2 & 3 ,can lead to confusion around further processing and the issues that need to be considered under the second principle.

Overall the DPA works well, and the issues are more in respect of other legislation that has been created to complement and enhance information sharing – for example, S115 Crime and Disorder Act, Freedom of Information Act, Human Rights Act, Children’s Act, Housing Act. There is little clarity as to how this other legislation works with the DPA in terms of enabling information sharing, and under what circumstances each of these powers should be used.

Agreement between the Information Commissioners Office and the Police Service on the

interpretation of Section 31(2) (iii) (Regulatory Activity) would be beneficial. For example, some areas of the police service rely on this as an exemption to the disclosure of information on disciplinary files, on the basis of the service being “persons authorised”, a view not shared by the Information Commissioners Office.

#### Question 10.

Comments: As explained at Question 9, the second principle of the Data Protection is being overlooked due to over reliance of Schedules 2 & 3 under the First Principle.

#### Question 11.

Comments: Due to the complexity of the Act, the only barrier that stands in the way of the effectiveness of the DPA is that individuals get immersed in the detail and are not taking a pragmatic approach to its application, therefore overlooking the basic principles contained within the legislation.

#### Question 12.

Comments: The view of the police service is that no sweeping changes are necessary at this time. Adherence to and application of the Data Protection Act was considered within the Bichard Inquiry which concluded that no revision was required in response to the events leading up to the Soham murders. The Bichard Inquiry quoted a member of the judiciary who referred to the Data Protection Act as an ‘inelegant and cumbersome’ piece of legislation, but Bichard concluded that the legislation was not the problem. The MoPI guidance meets the recommendation of Bichard for guidance on the collection, retention, deletion, use and sharing of information, so that police officers, social workers and other professionals can feel more confident in using information properly.

One area for consideration is that the DPA should include similar provision on charging for disbursements (photocopying, producing different format, postage etc) as the Freedom of Information Act. The current charge of £10 does not cover administration and search costs, therefore more extreme cases should incur additional fees.

#### Question 13.

Comments: The ACPO Criminal Records Office manages the United Kingdom Central Authority for the Exchange of Criminal Records (UKCA – ECR). This positive initiative was established under a European Framework Agreement which was developed in 2005. This has the responsibility to exchange criminal convictions between all 27 EU Member States and also provides an opportunity to exchange fingerprints when available.

There are other initiatives, such as Prum and G8, which include provisions to improve the

exchange of DNA and fingerprints.

The Human Rights Act can be a barrier to data sharing in the context of achieving policing objectives. For example, the Regulation of Investigatory Powers Act (RIPA) legislates for the acquisition and disclosure of data relating to communications.

The Criminal Justice and Police Act 2001 amended PACE removing the requirement to destroy DNA and fingerprints on acquittal or other discontinuance. As a direct result the police service now retains DNA and fingerprints from persons that have been acquitted, or case discontinued. This was the subject of challenge in the S & Marper case which was heard in the House of Lords and is now scheduled to be heard in the European Court in Strasbourg.

The Criminal Justice Act 2003 provided the police with the power to take DNA samples and fingerprints without consent from all persons detained at a police station having been arrested for a recordable offence. A record on PNC will contain relevant personal data and details of the offence which resulted in the record creation. This is an example of a positive piece of legislation and provides the police service with continuing access to data that will allow it to discharge its statutory and common law responsibilities. This was the subject of challenge in a recent EU case.

The Criminal Records Bureau was set up to ensure a comprehensive and effective means through which employers, voluntary organisations and others could obtain details of an individual's criminal history and background to assess suitability to work with children, vulnerable adults and in positions of trust. Part V of the Police Act 1997 requires the disclosure of all convictions, cautions, final warnings and reprimands held on Central Records (PNC). This creates a tension particularly as the police now retain information on PNC until an individual is deemed to have attained 100 years of age.

#### Question 14.

**Comments:** There is no power for the Police to demand the 'Nationality' or other identifying features from a subject, for example a National Identification Number, such power would be beneficial in meeting our responsibilities under the CRB Framework Agreement (Q. 13 refers).

Generally the view of the Police Service is that additional statutory powers would not necessarily or conclusively enable better and more secure sharing of information.

Knowledge and information are recognised as being valuable resources and at the heart of this recognition is an acknowledgement that the public sector needs to make the best use of them. The public sector is already required to adopt coherent and compatible information policies in support of better policy making, better service delivery and more efficient working. Commitment to this e-Government strategy will ensure the sharing of personal and operational information meets citizen and HMG expectations regarding accessibility, convenience and security.

A wider uptake of effective and approved Public Key Infrastructure (PKI) solutions coupled with the continued and expanded use of trusted infrastructures, for example the Government Secure Intranet (GSI), Criminal Justice Extranet (CJX), Criminal Justice Secure Mail (CJSM) and the Secure Communities Network (SCN) will continue to enable better and more secure

information exchanges.

Question 15.

Comments: The police service adopts a victim focussed approach but this is at times impeded by the processes required to enable the sharing of information with Victim Support, the requirement for consent in this context places an unreasonable burden on operational policing. It is time consuming, and can be distressing for a victim. A practical approach would be that in all cases the information may be shared with appropriate voluntary bodies unless the person expressly states their wish as otherwise.

The requirement under the data Protection Act 1998 to provide a Subject Access Facility for data held on the PNC presents a heavy burden on the Police Service. As referred to at Q12, the current administrative fee of £10 does not support this activity, particularly as it is paid directly into central funds. Moreover, the Police Service has identified that many of these requests, far from being genuine subject access requests, are on behalf of third parties for either employment vetting or Embassy Visa applications. Acknowledging that Section 56 of the data Protection Act will outlaw the practice of third party subject access checking, the Police Service have put in place an arrangement for proving Police Certificates for the purposes of obtaining an Embassy Visa which now sits outside of the Subject Access arrangements. This is in the form of a pilot which commenced in January 2008 and is already proving hugely popular with the public and Embassies and also police forces throughout the country.

**Section 4: Consent and transparency**

Question 16.

Comments: As stated above at 15, the sharing of information with Victim Support is based on 'informed consent'; however it is sometimes perceived as unclear how this consent should be obtained and recorded. It is our view therefore that a clearer distinction between our duty to obtain consent or informing individuals on how the information is being processed is required.

ACPO has initiated a review of the Volunteer DNA procedures. This review aims to ensure that individuals are providing genuine informed consent to load their profile to the National DNA Database (NDNAD) when they provide a sample. The work will also review existing profiles held on the NDNAD that were taken under the old arrangements.

Question 17.

Comments: The police service shares information without consent with partner agencies, a requirement to gain consent would place individuals at risk and prevent the police service discharging its statutory responsibilities. For example, Child Protection

The sharing of personal information is subject of safeguards, and based on establishing a

policing purpose or legal gateway, there should be no changes to the current position.

The main barrier for the police service in gaining consent would be the practicalities of doing so given the number of persons coming to notice within the course of police duties each day.

Question 18.

Comments: The introduction of Information Sharing Agreements under MoPI will go some way to providing the public with a clearer idea of the organisations with which we share information, and how this assists us in our fight against crime.

A requirement to publish Information Sharing Agreements on police internet sites would provide greater transparency.

Question 19.

Comments: Section 6 of the MOPI guidance provides clear guidance to the police service on the information sharing process and emphasises the importance of sharing police information with others.

ACPO will be undertaking a privacy impact assessment in respect of the Police Certificate initiative described in the response to Q .15.

## **Section 5: Technology**

Question 20.

Comments: Overall the police service welcomes technological advances in support of business processes to enhance data sharing. However there are inherent risks in using technology, particularly when its use is designed to provide solutions ahead of fully developed business requirements.

Sharing - Technological advances have enhanced the application of intelligence based policing principles at local force level.

At national level police forces are not able to effectively exploit their information assets, and are hampered by geographic and system boundaries. The IMPACT programme aims to deliver an effective integrated national, regional and local information sharing and intelligence capability, which will improve the ability of the police and partner agencies to proactively use information for intelligence purposes to prevent crime, bring offenders to justice, safeguard children and vulnerable persons, and further professionalise the investigation process.

Protection of personal information - increased access to personal information using technological advances inevitably leads to an increased risk of leakage and misuse. The police service seeks to reduce such risk through information compliance procedures and robust application of misconduct procedures, criminal investigation of members of the service suspected of misuse. Technological advances enable Professional Standards

Departments within the police service to conduct effective investigations of alleged breaches of information security by members of staff eg monitoring of use, audit trails, covert flagging of records.

Question 21.

Comments: The view of the Police Service is that there is no requirement (indeed it might prove unnecessarily proscriptive, expensive and resource intensive) for the law to mandate specific technical security controls / safeguards to protect personal and other operationally sensitive information.

There is currently a Pan Government review of all (not just technical) security measures required to protect personal information in order to restore public confidence. The Police Service (through the National Policing Improvement Agency) is required to respond to the review and affirm that there are adequate protective security controls in place to meet revised security arrangements for personal and other operationally sensitive information stored on media removed from secure premises.

Specifically, the review will focus on all protective measures for information at rest on laptop computers and other mobile computing devices, information in transit, information stored on, or transferred to exchange media devices, e.g. memory sticks, CD-ROMs and DVDs and information exchanged with criminal justice and other partners.

It is intended that the review should measure the effectiveness of protective measures against the standards outlined in HMG Manual of Protective Security (MoPS), Communications Electronic Security Group (CESG) Information Security (Infosec) Standards 1,2,3,4 & 5, CESG Infosec Memoranda 30, 34 and 35, CESG Good Practice Guide No. 5 (Issue 1.1 – January 2008) and Industry Best Practice Guidelines (BS / ISO 27001:2005). The results will indicate how security measures, particularly encryption products, have been deployed. Senior Information Risk Owners (SIRO) and Information Assurance (IA) Champions in Forces will be required to satisfy themselves that there are adequate protective security measures in place and that there are programmes of work in place to manage / treat identified risks to acceptable levels if / where protective security arrangements are identified as being inadequate.

Furthermore, the results of the review will be invaluable in compiling the national response both to HMG and others requesting information, e.g. under Freedom of Information legislation, and will provide reassurance to the public.

Question 22.

Comments: The police service publishes crime and disorder information to the public on force websites, the information is sanitised to protect the identity of victims and households.

## **Section 6: International comparisons**

### **Question 23.**

**Comments:** With reference to the work described at Q 13 regarding the EU wide sharing of conviction information, the UKCA-ECR are engaged in a pilot arrangement with 11 other member States to electronically share information which will be coded to ensure efficiency.

### **Question 24.**

**Comments:** The ACPO Criminal Records Office, in their management of the UKCA-ECR are building their knowledge and currently exploring this area and have proposed the creation of an emerging issues forum within the context of their work.

### **Question 25.**

**Comments:** As a result of the Framework Agreement described at Q13 above, all 27 Member States are committed to sharing conviction extracts and fingerprint data where available. Additionally, some non-EU Member States, such as Switzerland are also keen to begin fingerprint exchange in support of conviction exchange under the 1959 European Convention on Mutual Assistance in Criminal Matters. This has assisted in identifying criminals and other dangerous persons residing in countries other than their country of Nationality. This helps to prevent crime, protect the public and in some cases helps to eliminate the innocent.

An excellent working practice introduced during the past year is UKCA Criminal Exchange Office based in Hampshire. This followed from an agreement from EU countries with regard to the exchange of previous convictions between the member states without the requirement for an International Letter of Request, known as a Commission Rogatoire in Europe. A process which previously took 6 months+ is now usually attainable within 2 to 10 working days.

International Liaison Enquiry Team (ILET) encounters data protection issues with Law Enforcements Agencies worldwide on a daily basis. Seeking information through national agencies, such as Interpol, is time consuming due to ensuring compliance with data protection. The Hampshire Constabulary plays an integral part in the Cross Channel Intelligence group which involves the Belgian, Dutch, French and UK police forces which enables intelligence and information sharing on a "police to police" basis. This process is also mirrored by way of the Lingaunet usergroup, Linguanet being a computer based system that is currently in use at over 50 sites throughout Europe, this system allows simple low level cross border checks to be undertaken.

The fact that UK is not yet a member of the Schengen Information System (SIS) restricts the ability of UK police forces with regard to intelligence checks on the SIS database.

### **Question 26.**

**Comments:** Under Part V of the Police Act 1997, the UK use data held on the PNC for employment vetting purposes. The Criminal Records Bureau (CRB) are also keen to use information that is obtained from other EU Member States but there appears to be little appetite in other EU Member States for sharing such data for this purpose.

**Section 7: Additional questions**

Question 27.

Comments: No.

Question 28.

Comments: Following the creation of a Criminal Records Office by ACPO, a focal point has been provided for a range of other agencies such as the Borders and immigration Agency, the Identity and Passport Service and HM Prison Service to share data for the purposes of law enforcement and public protection.