

Collection and Storage of Personal Information

Driver – Political, Social, Technology, Legal

Related Drivers – Equality, Diversity and Human Rights, Forced Marriage and ‘Honour’-based Violence, Mental Health, Organised Crime, Counter Terrorism, E-crime, Fraud, Increasing Accountability, Reducing Bureaucracy, Violent Crime – Domestic Violence, Violent Crime – Sexual Violence, Violent Crime – Gun and Gang Related Violence, Violent Crime – Knife Crime

Background

This section focuses on the collection, storage and usage of personal information to prevent and combat serious crime and terrorism. In particular, it focuses on recent developments in the areas of the National DNA Database (NDNAD), Police National Computer (PNC) and Interception Modernisation Programme (IMP).

Political Context

In response to the European Court of Human Rights (ECHR) ruling (see [Legal Context](#)), the first in a series of DNA database consultations were launched. ‘*Keeping the right people on the DNA database*’ suggests a change to the current guidance on how long DNA records are retained and is open to consultation until 7 August 2009. Some of the changes include:

- Destroying all DNA samples like mouth swabs, hair or blood as soon as they are converted into a profile
- Automatically deleting the DNA profiles of anyone arrested but not convicted of serious violent or sexual crimes after 12 years
- Automatically deleting the DNA profiles of anyone arrested but not convicted of all other crimes after six years
- Removing the DNA profiles of young people arrested but not convicted (or convicted for less serious offences) when they turn 18
- Retaining indefinitely the DNA profiles and fingerprints of anyone convicted of a recordable offence¹

The Government intends to bring forward proposals for a consultation on the retention arrangements for DNA profiles in a Forensics White Paper to be published later in 2009, which will include:

- Varying the timescale of retaining DNA evidence dependent upon the seriousness of the offence, the age of the individual and the degree of risk posed by the individual
- Re-examination of the current retention arrangements for DNA profiles

- Ensuring that the police can retrospectively take samples for a longer period after conviction and from those individuals who are convicted overseas.²

Home Secretary, Alan Johnson has ordered a review of the Police National Computer (PNC) to propose guidelines on what records should be held, for how long and for what reasons.³ Under the current policy records remain on the PNC for up to 100 years. Criteria could include the extent of the penalty handed out, how long the offence was committed, the age of the defendant and whether or not they reoffended. Records from serious, violent and sexual offenders, would stay on the register. This work will be carried out by an independent advisor to be appointed at the end of summer 2009. The announcement has raised concerns that low level offenders could escape detection in future because the pattern of their early criminality has been erased. The review is linked to a case before the Court of Appeal in which five chief constables are challenging a ruling that holding details of minor offences for long periods breaches data protection rules.

The Government, in April 2009, launched plans for their Interception Modernisation Programme (IMP). Telephone companies and internet service providers already retain 'communications data' for all their customers for a period of 12 months. Under Home Office proposals, mobile and fixed line operators, or communication service providers (CSPs), will be required to process and link the data together to build complete profiles of every UK internet user's online activity. Police and the intelligence services would then access the profiles, which will be stored for 12 months, on a case-by-case basis. Approximate costs associated with this programme are £2bn and legislation underpinning it will be written into the Communications Data Bill (see [Legal Context](#))

The Government are consulting (until 20 July 2009) on the IMP plans in the consultation '*Protecting the public in a changing communications environment*'. This lays out the plans for the IMP which proposes a "middle way" requiring CSPs to retain the information. Previously, plans for a centralised government database were suggested but ruled out on privacy grounds.⁴ Summary of the proposals in the consultation are as follows:

- Legislation to ensure all data that public authorities might need, including third party data⁵ be collected and retained by CSPs such as the fixed line, mobile and WiFi operators.
- Having CSPs process the data to enable specific requests by public authorities – such as the police and Security Service - to be processed quickly and comprehensively.⁶

The All Party Parliamentary Group on Privacy is going to probe the IMP in July 2009. The group was formed to offer "early warning protection" on privacy issues.⁷ Its membership is drawn from MPs and peers on all sides of both Houses and includes David Davis and Lord Carlile, the independent scrutineer of terrorism legislation. The Home Office said it would cooperate with the Group on Privacy's work.

Social Context

Last year the Information Commissioners Office (ICO) investigated five complaints about the retention of old conviction data and concluded that the data was no longer relevant and was excessive for policing purposes. Under the Data Protection Act 1998, personal information processed for any purpose should be adequate, relevant and not excessive and should not be kept for longer than is necessary for that purpose. The ICO issued enforcement notices to the forces to delete the material but the police appealed.

Two individuals, S. and Marper took the UK Government to the European Court of Human Rights (ECHR) over the police's refusal to destroy their fingerprints and DNA samples after unsuccessful criminal proceedings. The ECHR judges said "*the retention in question constituted a disproportionate interference with the applicants' right to respect for private life and could not be regarded as necessary in a democratic society*".⁸

It was widely expected that the DNA profiles, samples and fingerprints of 850,000 innocent people kept on the database would be destroyed in response to the ruling. But the proposals outlined in the consultation, '*Keeping the right people on the DNA database*' fall short of those expectations by retaining records of those not convicted for 6 – 12 years depending on the crime. This contrasts with the situation in Scotland, where only the DNA profiles of suspects arrested for serious violent and sexual offences are retained for a maximum of five years.⁹

Human rights groups, and opposition politicians have expressing dismay that the Home Office had rejected that option and predicted a race to the courts to challenge the new policy:

"The government just doesn't get this," said the shadow home secretary, Chris Grayling. The Liberal Democrats' Chris Huhne added: "*This is an undignified rearguard action designed to give as little as possible.*"

Liberty's Shami Chakrabarti said: "*Wholly innocent people – including children – will have their most intimate details stockpiled for years on a database that will remain massively out of step with the rest of the world.*"¹⁰

An independent report published by the Human Genetics Commission (HGC), '*Citizen's Inquiry into Forensic Use of DNA and the DNA National Database*'¹¹ looked at the public's views on the development of the national DNA database and, in particular, whether storing the DNA profiles of victims and suspects who are not charged or are subsequently acquitted is justified by the need to fight crime. Most participants, although not all, felt that it would not be practical or desirable to have the whole population registered on the database.

The Nuffield Council on Bioethics report, '*The forensic use of bio-information: Ethical issues*' considers whether current police powers in the UK to take and retain bio-information are justified by the need to fight crime.¹² In general the report agrees that the authority to take (for impending use in criminal investigation) fingerprints and biological samples without consent from those who are arrested on suspicion of involvement in any recordable offence is proportionate to the aim of detecting and prosecuting crime. It, however, is against the

police being permitted to take and store both fingerprints and biological samples from all arrestees without their consent, regardless of the reason for the arrest. In all other cases, samples should be destroyed and the resulting profiles deleted from the National DNA Database (NDNAD).

A briefing by the Policy Engagement Network at the London School of Economics and Political Science (LSE) recently examined the Interception Modernisation Programme (IMP) consultation, '*Protecting the public in a changing communications environment*'. The LSE's academics questioned whether the government had fully appreciated the legal and democratic implications of IMP. They said thousands of planned Deep Packet Inspection (DPI) probes to harvest data on web browsing, email, VoIP calls and instant messenger conversations from inside ISP networks would blur the legislative and ethical lines between communications data and communications interception. The authors as well as other members of the public have criticised the scheme for its extension of intelligence-service powers.¹³

Because of this report, the All Party Parliamentary Group on Privacy has launched an investigation into IMP.

Technology Context

Most of the proposed 10-year budget for the system would be spent on Deep Packet Inspection (DPI) equipment that would allow CSPs to tap into third party communications data carried by their networks. Additionally the government plans to order CSP to "not only to collect and store data but to organise it, matching third party data to their own data where it had features in common"

The London School of Economics briefing makes the point that beyond the challenges of building a DPI system that can collect this information at speed and evolves side by side with changing technology without becoming redundant, is what is done with the information once it is collected. For instance:

- DPI may be able to detect the fact that there is some form of criminal activity, but additional processes would be necessary to go after the suspects. These may include content interception or investigative work to interpret the communication data, and understand what physical or social process maps to this particular pattern or network use.
- While a large fraction of the population will be easy to identify, a significant fraction of people, particularly those involved in suspect activities and using surveillance countermeasures, will always be difficult to identify or detect.

The briefing goes on to say "*for finding and identifying the fraction of users of interest to law enforcement and what exactly they are up to, we will still need the police to do policing work.*" Collecting communications data is only one aspect of the investigation. In terms of what can be presented in court and linked to specific individuals are hugely significant. At the moment UK law enforcement has about 300 police officers in formal High-Tech Crime Units and employs overall between 500-600 specialist computer forensic examiners, a mix of

police officers and civilian employees. In most police forces there are backlogs in excess of six months for “non-urgent” (i.e. where there is no immediate threat to life or serious conspiracy in progress) examinations.

Regarding the DNA database, the proposed changes to DNA data retention will effect how the police currently collect and handle DNA, process, retain and use the database.

Legal Context

The Information Tribunal has dismissed appeals by Humberside, Northumbria, Staffordshire, Greater Manchester and West Midlands Police and ruled that the **retention of the old convictions data** is in breach of the **Data Protection Act 1998**. The five forces have as a result been ordered to delete old criminal convictions from the Police National Computer (PNC).¹⁴

The European Court of Human Rights (ECHR) made a ruling that the decision to continue storing fingerprints and DNA samples taken from applicants after unsuccessful criminal proceedings against them were closed was a breach of human rights in the case of *S. and Michael Marper v. the United Kingdom*.

In this case both applicants requested that their fingerprints and DNA samples be destroyed. These requests were rejected and after their appeal was thrown out by the House of Lords, they took it to the European Court on Human Rights. Both applicants stated that the retention breached their Article 8 ECHR rights (right to respect for private and family life) and Article 14 ECHR rights (prohibition of discrimination).¹⁵

In response to the court ruling, new standards for the use of investigatory powers and retention of DNA profiles were outlined for public authorities on how and when DNA profiles are to be retained on the national database. New draft Codes of Practice were published to replace existing Covert Surveillance and Covert Human Intelligence Sources to provide better clarity on when the use of RIPA technique is proportionate.¹⁶ Further changes to data retention will follow after the Forensic White Paper is published later in 2009 (see [Political Context](#)).

However the consultation ‘*Keeping the right people on the DNA database*’ shows the Government is not going to fully comply with the ECHR ruling that all records of those who are innocent are deleted from the database, instead they will be retained 6 – 12 years depending on the severity of the crime they were not convicted. Home Office ministers say their ‘proposals in the consultation do comply with the landmark *S. and Marper* judgment in Strasbourg which declared unlawful their policy of keeping all unconvicted suspects’ DNA profiles indefinitely because of its “blanket and indiscriminate” nature.

The EU Data Retention Directive, requires that Communications Service Providers (CSPs) store communications traffic data for between 6 months and 2 years (depending on how the Member State wishes to implement the Directive - it is likely that the UK will go for 12 months). The Directive covers fixed telephony, mobile telephony, Internet access, Internet email and Internet telephony. Member States are required to transpose it into national law within 18 months. However, they may if they wish, postpone the application of the Directive

to Internet access, Internet email and Internet telephony for a further 18 months after this date. The UK indicated that they will indeed exercise this option.¹⁷

The Communications Data Bill, part of the draft legislative programme 2008/09, will implement the remainder of the European Union's Data Retention Directive.¹⁸ The Bill will potentially contain legislation underpinning the Interception Modernisation Programme (IMP) (see [Political Context](#)).

Current legislation governing surveillance - the Regulation of Investigatory Powers Act (RIPA) - draws a strong distinction between communications data and communications interception. The former requires only the approval of a senior law enforcement or intelligence officer, the latter a warrant signed by the Home Secretary. Officials aim to maintain the separation if IMP is implemented.

Passage of the IMP programme would mean large numbers of requests for what might be considered authorisations for "communications data" would need to be converted into requests for "intercepts". As the product of interception is currently inadmissible a number of new problems for investigators and prosecutors about what they can use in evidence and what they are required to disclose under Criminal Procedures and Investigations Act arise.

The Government are currently consulting on the IMP programme through the '*Protecting the public in a changing communications environment*'. Results from the consultation will have legislative impact if the programme is taken forward.

Potential Skills Needs

Analytical skills – to visualize, articulate, and solve complex problems and concepts, and make decisions that make sense based on available information

Collaborative working skills – working effectively with colleagues, partners and other agencies

Computer forensic skills – analysis of information contained within and created with computer systems and computing devices, typically in the interest of figuring out what happened, when it happened, how it happened, and who was involved

Data collection and management skills – recording and collecting data in line with a particular system

Data recording skills – recording information in an appropriate format

Information sharing skills – to provide effective information to partner agencies

Intelligence gathering skills – to scan multiple data sources and follow leads

Intelligence information sharing skills - between police forces and other intelligence and security agencies

Inter-agency working skills – to work effectively with two or more governmental agencies

IT skills – general awareness and understanding of current ICT environment and changing landscape

Multi-agency working skills – to work with other agencies to protect UK borders

Partnership working skills – to work effectively with other agencies to a common goal and standards

Risk management skills- to manage and mitigate risk

Strategic leadership skills - to provide a clear vision and sense of purpose

¹ [Home Office \(2009\) Consultation: *Keeping the right people on the DNA database*. Start date 7 May 2009, Finish date 7 August 2009.](#)

² [NPIA \(February 2009\) *NPIA Digest*. London: NPIA p18](#)

³ [Police Oracle Online, 23 June 2009, 'New Home Sec orders immediate review of PNC'.](#)

⁴ [Home Office Press Release, 27 April 2009, 'Government launches consultation on communications data and ruling out single store'.](#)

⁵ Third party data is data generated by communications services based overseas but crossing the networks in the UK.

⁶ [Home Office \(2009\) Consultation: *Protecting the public in a changing communications world*. Start date: 27 April 2009, End date: 20 July 2009.](#)

⁷ <http://www.privacyappg.org.uk/>

⁸ [BBC News Online, 4 December 2008, 'DNA Database 'breach of rights'.](#)

⁹ [Criminal Justice and Licensing Bill \(Scotland\)](#)

¹⁰ [The Guardian Online, 7 May 2009, 'Ministers keep innocent on DNA database'](#)

¹¹ [Murtuja, B., Adris, K., & Ahmed, J. \(2008\) *Citizen's Inquiry into Forensic Use of DNA and the DNA National Database*. London: Human Genetics Commission.](#)

¹² [Nuffield Council on Bioethics \(2007\) *The forensic use of bio-information: Ethical issues*. Cambridge: Cambridge Publishers Ltd.](#)

¹³ [Policy Engagement Network \(2009\) *Briefing on the Interception Modernisation Programme*. London: London School of Economics and Political Science.](#)

¹⁴ [Information Tribunal Appeal EA/2007/0096,98,99,108,127 Chief Constables vs Information Commissioner](#)

¹⁵ [NPIA \(April 2008\) *NPIA Digest*. London: NPIA p31](#)

¹⁶ [NPIA \(May 2009\) *NPIA Digest*. London: NPIA p11](#)

¹⁷ [Official Journal of the European Union, L 105, 13.4.2006, p 54 and 61.](#)

¹⁸ [Communications Data Bill \(UK\)](#)