LIBERTY

PROTECTING CIVIL LIBERTIES
PROMOTING HUMAN RIGHTS

Serious Crime Bill

Liberty's Briefing and Amendments for Committee Stage in the House of Lords (Part III – Data Sharing and Mining)

March 2007

About Liberty

Liberty (The National Council for Civil Liberties) is one of the UK's leading civil liberties and human rights organisations. Liberty works to promote human rights and protect civil liberties through a combination of test case litigation, lobbying, campaigning and research.

Liberty Policy

Liberty provides policy responses to Government consultations on all issues which have implications for human rights and civil liberties. We also submit evidence to Select Committees, Inquiries and other policy fora, and undertake independent funded research.

Liberty's policy papers are available at
http://www.liberty-human-rights.org.uk/publications/1-policy-papers/index.shtml

Parliamentarians may contact:

Gareth Crossman
Director of Policy
Direct Line: 020 7378 3654
Email: GarethC@liberty-human-rights.org.uk

Jago Russell
Policy Officer
Direct Line 020 7378 3659
Email: JagoR@liberty-human-rights.org.uk

Introduction

1. There is no doubt whatsoever that serious crime causes human misery and massive cost to society (financial and otherwise).[1] The state has a moral responsibility to take steps to combat serious crime. What these individual steps should be and where we should allow them to take us in the long-term is, however, an entirely different matter. This is where Liberty sometimes, though not always,[2] parts company with the Government. Liberty's proposed amendments are not designed to undermine the ability of the state to tackle serious crime. Instead, we hope they will help Parliament to scrutinise whether the measures in the Bill are really necessary and whether they are likely to work. We also hope they will give parliamentarians the opportunity to debate whether serious crime could be tackled in a way which does less damage to our democratic values, our human rights and the rule of law.

2. The amendments proposed in this briefing relate to Part III of the Bill.[3] Part III proposes, amongst other things, increased data sharing powers across public and private sector bodies for the purposes of identifying and preventing fraud. It would also give express statutory authorisation to the practice of data matching (or data mining) which involves computerised fishing expeditions into the personal data of huge numbers of people, most of whom there is no reason to suspect have been involved in any kind of fraudulent activity. The Audit Commission is already conducting data matching exercises on a bi-annual basis to identify fraud (the National Fraud Initiative). We urge Parliament not to give a green light to this practice without first considering its privacy implications. We hope Parliament will also focus on how Part III would increase the scope of the existing practice of data matching, including by (a) giving the Home Secretary the power to extend the purposes for which data matching can be undertaken; (b) increasing the involvement of private bodies in data matching exercises and; (c) amending the terms of the Data Protection Act 1998.

---

[1] Recently uncovered people smuggling operations have, for example, shown the horrific, sometimes lethal, conditions that people are forced to endure at the hands of smuggling rings (http://news.bbc.co.uk/1/hi/england/london/5405870.stm)

[2] We agreed, for example, with the setting up of the Serious Organised Crime Agency (SOCA).

[3] We have proposed amendments to Parts I and II of the Bill (see http://www.liberty-human-rights.org.uk/publications/1-policy-papers/index.shtml).

3. This kind of mass data collection, data sharing and data mining is a familiar theme in Home Office legislation, raising serious ethical and constitutional issues. Government schemes that interfere with personal privacy, such as the DNA Database and ID Cards, involve less tangible rights infringements than measures, like Gangster-ASBOs, which deny people a fair trial. However, when one aggregates the impact of such schemes across the millions of people they affect, the real extent of the privacy infringement becomes clear. These schemes have the potential to change the nature of the relationship between state and citizen, turning us from a nation of citizens into a nation of suspects.

***

Amendment 1 – Suspected Fraudsters

Clause 61, page 32, after line 37 insert –

"(c) is personal data, within the meaning of section 1 of the Data Protection Act 1998 (c.29), pertaining to a person who the public authority does not suspect of involvement in fraud."

Schedule 6, page 65, after line 14, insert –

"(5) But nothing in this section authorises or requires a disclosure which –

(a) contravenes the Data Protection Act 1998 (c.29),

(b) is prohibited by Part 1 of the Regulation of Investigatory Powers Act 2000 (c.23), or

(c) is personal data, within the meaning of section 1 of the Data Protection Act 1998 (c.29), pertaining to a person who the public authority does not suspect of involvement in fraud."

Schedule 6, page 65, after line 37, insert –

"(c) is personal data, within the meaning of section 1 of the Data Protection Act 1998 (c.29), pertaining to a person who the public authority does not suspect of involvement in fraud."

Effect

4. As a result of this amendment, the Bill would only authorise the sharing of personal data if this pertains to a person who is suspected of involvement in fraud. The amendment would place no additional restrictions on the sharing of non-personal data. The amendment would also ensure that the Audit Commission's powers to require a body to disclose information does not displace any restrictions on the disclosure of information under the Regulation of Investigatory Powers Act 2000 and/or the Data Protection Act 1998.

Briefing

5. The mass data sharing and data mining that Part III of the Bill would authorise is indicative of a general shift in the state's approach to the taking, retaining, sharing and automated searching of our personal data (cf ID Cards, DNA Database and the Children's Index). This is done not because the information in question is believed to be of use or because the person it relates to is thought to have done anything wrong. It is done because this information *might* be of use at a future point or because when the state looks at the information it *might* find that we have done something wrong.[4] This new approach to our personal information raises profound ethical issues and questions about the proper relationship between the state and the citizen. At Second Reading Lord Thomas of Gresford likened these data sharing and data mining powers to a "high-tech version of the writ of assistance" because "[i]t is not necessary for there to be evidence of wrongdoing, a probable cause or a warrant based on reasonable suspicion".[5] This approach to personal privacy treats people not as citizens but as suspects.

6. The sharing and use of personal information engages a person's right to privacy. We believe that it should therefore be (A) justified (is there a legitimate reason for the intrusion of privacy in question?) and (B) proportionate (could that legitimate aim be

[4] This has only become possible due to huge technological advances in recent years. Until recently it would have been very difficult to foresee this happening or, at least, to suggest it without being dismissed as a "conspiracy theorist".

[5] HL Deb, 7 Feb 2007, col 738 ff

achieved in a way which does not intrude into a person's privacy or does so less?)[6] It is clear that tackling fraud is a legitimate reason for some infringements on personal privacy. As the Government rightly and repeatedly explains, fraud costs the state millions of pounds. It is, however, difficult to see how it can be proportionate to infringe the privacy of millions of people on the off chance that a few hundred or even thousand cases of fraud will be identified. Undoubtedly data mining may help to identify some people that are involved in fraudulent activities but can identifying a few criminals really justify the state trawling through all of our personal data? The Government itself has acknowledged that there are concerns about the legality of the mass and indiscriminate mining of personal information to which the Bill would give statutory authorisation.[7]

7. This does not, however, mean that the state could never share and search personal information in order to identify fraud. The Data Protection Act 1998 ("DPA") and the protection of personal privacy under Article 8 of the European Convention on Human Rights 1998 provide a flexible and reasonable legal framework which permits private information to be used to combat crime. This should not, however, be done on an indiscriminate basis. It should, instead, be limited to the sharing and searching of personal information relating to those who are suspected of fraud. The targeted use of intelligence-sifted information would be a justified *and* proportionate response to fraud.[8] Sadly, the Bill does not limit the sharing and searching of personal information in this way.

8. We fear that the Government has been somewhat disingenuous in suggesting that this would be the case. It has given the misleading impression that it is only those who have something to hide who would be affected by these proposals. At Second Reading, Baroness Scotland commented "[i]mportantly, we will ensure that the

[6] Any sharing of personal data is likely to engage a person's right to privacy under Article 8 of the Human Rights Act 1998 (HRA). Under Article 8 (2) sharing can be justified on the basis that the sharing is authorised by law, serves a legitimate purpose (such as preventing crime or protecting the economic well-being of the country) and is not excessive.

[7] Home Office Consultation: *New Powers Against Organised and Financial Crime*, July 2006, Page 22

[8] For example, if there is reason to suspect that a person has committed fraud, it would be justified for relevant information about that person to be shared with the police or other investigating authority to help determine guilt. That type of targeted information sharing would come within the scope of permissible data sharing under Schedule 2 and 3 of the DPA or which could be permissible under the crime and taxation exemption contained in Section 29 of the Act.

provisions are used to target suspected fraudsters *rather than simply those who are potential fraudsters*" [emphasis added].[9] The Home Office has also published a document stating:

> "Respondents cited problems with the existing data sharing gateways and so the Government intends to legislate to create a general power to allow cross-sector data-sharing *on fraudsters* to take place" [emphasis added].[10]

These statements are misleading. It is not only fraudsters' personal data that would be shared and searched under these provisions. Bodies engaging in the anti-fraud exercise in question (whether a Central Government Department, NHS body or even a private bank or insurance company) would be required or authorised to share personal information relating to many thousands or millions of people. The vast majority of these would in no way be suspected of fraudulent behaviour.

***

Amendment 2 – Sensitive Data

Clause 64, page 35, line 43 – stand part

Effect

9. Clause 64 would amend the Data Protection Act 1998 so that the prevention of fraud is included in the Act as another legitimate reason for the processing (i.e. disclosing or mining) of sensitive data. This amendment would delete that Clause, with the effect that sensitive data could only be processed if it falls within another existing ground contained in Schedule 3 of the 1998 Act (i.e. it is necessary for the administration of justice (para 7(1)(a)) or the data subject has given his/her explicit consent (para 1)).

[9] HL Deb, 7 Feb 2007, col 732

[10] Home Office, "New Powers Against Organised and Financial Crime – A Summary of Responses", November 2006, p.6

Briefing

10. Clause 64 of the Bill indicates that it is not only relatively innocuous personal data but also sensitive data that will be subject to the mass data-sharing regime envisaged by the Bill. This could include information about one's racial or ethnic origin, political opinions, religious beliefs, physical or mental health and sexual life.[11] The Data Protection Act 1998 imposes special safeguards in respect of this sensitive information which means that it is only fair and lawful to process it[12] where one of a limited range of conditions is satisfied.[13] These include where the processing is necessary for the administration of justice[14] or where the data subject has given his/her explicit consent.[15] Clause 64 would add, as an additional justification for the processing of sensitive information, the prevention of fraud. As a result, if the sharing or use of sensitive personal data were part of an anti-fraud initiative, it would not need to be shown that any of the existing conditions for the processing of sensitive data in Schedule 3 are met.

11. It is unclear why the Government wants this express power to process sensitive data. It could be because this kind of information will help to identify whether someone is involved in fraud. This would, however, seem unlikely given the types of information covered by the definition of "sensitive information" - how could a person's sexual life or religious beliefs help to show whether they have been involved in fraud? Furthermore, one would imagine that if the processing of sensitive information were necessary for this reason, an existing condition in Schedule 3 of the Act would apply, i.e. the administration of justice.

12. We fear that this provision might, in reality, be included because it would simply be too difficult in practice to separate out this kind of sensitive information from non-sensitive information contained in a single source of data, access to which would be shared under these proposals. This could, for example, arise if the "data

[11] Section 2 of the DPA
[12] As required by the first data protection principle
[13] Schedule 3
[14] para 7(1)(a)
[15] para 1

sharing" involved access being given to a pre-existing database (like the Children's Index) containing both sensitive and non-sensitive data. If this is indeed the reason for this change to the DPA, we would be very concerned. Administrative convenience is not a sufficient justification for the sharing and searching of sensitive personal data.

13. Clause 64 also sits somewhat uncomfortably with the Government's repeated statements that Parliament need not be concerned about the provisions of Part III because they are all subject to the Data Protection Act 1998.[16] As this Clause demonstrates, these proposals would in fact change the content of the 1998 Act and affect the way it applies to data sharing and data matching. When summing up at Second Reading Baroness Scotland also seemed to express some reservations about whether the provisions of the Bill had an acceptable impact on data protection law: "We … are *relatively* assured that what is proposed in the Bill does not trespass inappropriately on the data protection provisions." [emphasis added][17]

***

Amendment 3 – Data Mining and Data Matching

Schedule 6, page 64, delete from after "match" on line 22 to end of line 23.

Effect

14. This would amend the definition of "data matching" so that it is restricted to "the comparison of sets of data to determine how far they match". It would no longer be defined as including the "identification of patterns and trends".

Briefing

15. One of Liberty's greatest concerns about the privacy implications of the Bill relate to the "data matching" provisions in Schedule 6. These would give the Audit Commission the power to conduct "data matching" exercises or to contract with other

[16] cf HL Deb, 7th Feb 2007, col 766, per Baroness Scotland
[17] Ibid

bodies, private or public, to do so on its behalf.[18] It would require bodies that are subject to audit by the Commission to provide information for the purposes of these exercises.[19] Schedule 6 would also empower bodies, whose accounts the Commission does not audit, to provide information for the purposes of data matching. This could include central Government departments, which, under these provisions, could theoretically provide access to the Children's Index or National Identity Register. Private bodies like banks, insurance companies and building societies would also be able to provide client details under the provisions of Schedule 6.[20] Information disclosed to the Commission for the purposes of "data matching" and the results of those fishing expeditions could be disclosed to an unrestricted range of bodies for fraud detection or prevention purposes or if there is another statutory duty to disclose the information.

16. This amendment seeks to explore what is really meant by "data matching" in this context. We hope that it will prompt the Government to explain what the Audit Commission is currently with the personal data of millions of people as part of the National Fraud Initiative and to describe what it might wish to do in the future with the mass of personal data that is being collected and shared.

17. "Data matching" could, on one level, involve little more than the comparison of two or more sets of data to see if there are overlaps – i.e. to ascertain whether same person or household appears in more than one of these data sets. This could, for example, identify someone who is claiming two benefits that are supposed to be mutually exclusive. This is what is suggested by the phrase "data matching". In reality, however, the definition of "data matching" goes much further. It is expressly stated to include "the identification of any patterns and trends".[21] We consider that this would in reality be more akin to data mining than data matching.

---

[18] Section 32A

[19] Schedule 6, para 2, proposed section 32B of the Audit Commission Act 1998 This would, for example, mean that local authorities, police authorities, probation boards, NHS trusts and primary care trusts could be required to make any databases they maintain available. The Bill imposes no restriction on the kinds of information that these bodies can be required to provide (which could, therefore, include patient records).

[20] Schedule 6, para 2, proposed section 32C of the Audit Commission Act 1998. This second group of bodies cannot provide information that is held for medical purposes.

[21] Schedule 6, para 2, proposed section 32A(2) of the Audit Commission Act 1998

18. Data mining involves the use of specialised software to 'profile' innocuous mass data in order to identify patterns or characteristics that might indicate some sort of unusual behaviour or impropriety. This is essentially a fishing expedition, which is not based on any suspicion or intelligence that a particular person or company has done anything wrong. The way data mining works can be illustrated by the following hypothetical example:

> *The Government wants to crack down on tax evasion and thinks the following factors are strong indicators that a person is engaged in this: (a) regularly paying with cash rather than credit cards or cheques, (b) having erratic streams of income, and (c) taking extravagant holidays. It sets up a computer programme that searches through all bank account statements, local authority and central government records and travel operator databases to identify these types of behaviour. The computer produces a list of every person who satisfies all three indicators and these people are then the subject of investigations by HM Revenue & Customs.*

As Baroness Anelay commented at Second Reading: "the Bill could open the way for operations under which software was used to search several databases to identify suspicious patterns of activity that simply could not be spotted when the data were seen individually."[22]

19. The consultation preceding the Bill acknowledged that there would be concerns about the legality of data mining.[23] We believe that this would raise difficulties over compliance both with DPA principles[24] and, in human rights terms, there will be proportionality issues arising from the fact that data mining, by its very nature, will not be targeted or intelligence sifted. In order to be effective[25] huge quantities of data would have to be analysed. Data mining may well help to identify some people that

[22] HL Deb, 7th Feb 2007, col 736

[23] Home Office Consultation: *New Powers Against Organised and Financial Crime,* July 2006, Page 22

[24] In particular the second principle that data 'shall be obtained only for one or more specified and lawful process', the third principle that 'data should be adequate, relevant and not excessive' and the fifth principle that 'data processed for any purpose…shall not be kept for longer than is necessary', page 18

[25] Presuming it is effective.

are involved in fraudulent activities but can identifying a few criminals really justify the state trawling through all of our personal data? As discussed above, we do not see how that this kind of random, computerised fishing expedition into our personal data can be proportionate.

20. Data mining could also give rise to serious practical concerns. As Lord Thomas commented at Second Reading:

> "It is the sort of thing that the supermarket card is designed to do to demonstrate to the management whether a customer buys buy tins of salmon or jars of Marmite. The patterns of behaviour thrown up by the data matching in Part 3 may or may not be meaningful; it is all a matter of chance. Depending on how they are interpreted, the Audit Commission will be able to point the finger at what is deemed to be a suspicious constellation of characteristics or behaviours in an individual. Instead of a system in which a person is suspected of a crime and is then investigated by the police, a trawl using the latest computer techniques will throw up names and those people will be investigated because of their characteristics or behaviours. Suddenly, we have grounds for a serious crime prevention order under Part 1."[26]

Many of us have experience of the inaccurate results thrown up by data mining exercises conducted into the information held about our shopping practices on supermarket loyalty cards. Data mining is clearly not infallible. Where it leads to a person being sent vouchers for a brand they would never, the data mining error is, perhaps, nothing more than an annoyance. If, however, it led to an innocent person being subjected to a police investigation or subjected to a "preventative" measure like a gangster ASBO the personal cost would be much greater an the risk of error, therefore, unacceptable.

21. Given these principled and practical concerns it is not surprising that other countries impose stringent safeguards on the ability of state bodies to mine personal data. Under German law, for example, stringent safeguards exist in relation to data mining for the purposes of investigating criminal offences. Data may only be mined for these purposes in the following circumstances and with the authority of the court:

[26] HL Deb, 7 Feb 2007, col 739 ff

- There must be evidence that a crime has possibly been committed;
- The crime in question must be a serious crime and one of the specific criminal offences set out in the criminal procedure rules (e.g. trafficking of drugs or weapons, a crime against the State, a crime which endangers the safety of the public, a crime that puts at risk life or limb, the sexual self-determination or personal liberty of an individual or finally a form of organized crime); and
- The investigation of the crime must be seriously impaired if the public authorities were denied the right to carry out a data mining exercise.[27]

As we discuss below, German law imposes even greater restrictions on the use of data mining to identify potential future behaviour. Liberty is concerned that no equivalent legal restrictions on data mining exist under UK law. We fear that parliamentary approval of data mining in the context of fraud prevention would be treated as a green light for the use of data mining processes in many other contexts.

***

Amendment 4 – Data mining and profiling

Clause 61, page 32, line 19, replace "prevent" with "detect"
Clause 61, page 32, line 20, replace "preventing" with "detecting actual or attempted"
Clause 61, page 33, line 12, replace "prevent" with "detect actual or attempted"
Clause 64, page 36, line 8, replace "preventing" with "detecting actual or attempted"
Clause 64, page 36, line 12, replace "prevent" with "detect actual or attempted"
Schedule 6, page 64, line 25, replace "prevention and detection of", with "detection of actual or attempted"
Schedule 6, page 68, line 18, replace "prevention and detection of", with "detection of actual or attempted"

[27] §98a *Strafprozessordnung*

Effect

22. As a result of this set of amendments the Bill would not authorise the sharing or mining of data for the purposes of *preventing* fraud or other forms of crime that have not yet been committed. It would not, however, prevent this being done to detect fraud or other criminal activity which has already occurred or which has been attempted.

Briefing

23. The practice of data mining envisaged by the Bill would involve the computerised searching of masses of personal data in order to identify "patterns or trends". As discussed above, Liberty has general principled and practical concerns about these proposals. We are particularly worried about these fishing expeditions being used to identify patterns, trends or profiles that suggest the possibility of *future* criminal behaviour. This would be permitted by Bill, which would authorise data sharing and data mining for the purposes of "preventing" fraud or other criminal behaviour; not merely investigating crimes and fraud which have already been committed or attempted. We do not believe it would be appropriate to mine data to predict the likelihood of fraud or other types of criminal behaviour with the aim of preventing them before they occur or are attempted.

24. Some patterns, trends or personal profiles, identifiable by a data mining exercise, might well suggest that a type of future behaviour is likely. We do not, however, believe that this should be used to justify "preventative" action, particularly where this could be detrimental in any way to the person concerned. Not everyone follows normal or typical patterns, trends or profiles. Just because a person grows up in an area where 9 out of 10 young people commit crime, it does not necessarily follow that s/he will follow suit. Individuals should be judged on the basis of what they do rather than what others like them have done in the past. Data mining to identify patterns of behaviour indicative of future risks will not be 100% successful. It would inevitably lead to innocent people being unjustly identified and targeted.

25. As discussed above, German law restricts the ability of the state to conduct data mining exercises to investigate crimes that have already been committed. Not surprisingly, it places even more stringent restrictions on the ability of state bodies to mine personal data in order to identify the possibility of future criminal behaviour. In a recent case the Federal Constitutional Court's considered an anti-terrorist initiative that involved each of the federal state's police forces to cooperate in relation to a Germany-wide data mining exercise with the objective of identifying *potential* Al-Qaida terrorists.[28] The Court found this operation to be unconstitutional and held that data mining for the purposes of crime prevention is only permissible if there is a clear and present risk to:

- the existence of the Federal Republic of Germany
- the security of the Federal Republic of Germany or one of its federal states, or
- the life, limb or liberty of an individual.

A general threat of a terrorist attack, as was assumed after 11 September 2001, or political tensions with a particular State were considered to be insufficient justifications. Thus, in order to mine data to prevent crime the German police authorities would have to demonstrate a clear and present danger of, for example, an imminent terrorist attack.

***

Amendment 5 – Information Commissioner

Schedule 6 Page 68, after line 9, after "32B(2)", insert, "the Information Commissioner's Office"

Effect

26. This amendment would require the Information Commissioner to be consulted before the data matching code of practice is drawn up or amended.

[28] BVerfG NJW 2006, 1939

Briefing

27. The Bill would require the Audit Commission to draw up and keep under review codes of practice on data sharing.[29] It is extremely important that the Information Commissioner is consulted on these and that they are agreed with him/her. The Government has itself acknowledged this. At Second Reading Baroness Scotland explained that the existing National Fraud Initiative "operates to a code of practice, on which the Information Commissioner has been consulted" and stated that this "will continue to be the case."

> "working with the Information Commissioner, we will be seeking to ensure that the arrangements are transparent and command public confidence, are proportionate and are subject to periodic review."[30]

We believe that this important role for the Information Commissioner should be a statutory requirement, included on the face of the Bill.

***

Amendment 6 – Extension of Purposes

Schedule 6, page 68, delete lines 12 to 21

Effect

28. This amendment would require primary legislation to be passed by Parliament to add further purposes for which data matching/mining may be undertaken.

Briefing

29. At present the only purpose for which data matching may be conducted is "the prevention and detection of fraud".[31] The Bill would, however, also confer a power on the Secretary of State to extend the purposes for which data mining may be

[29] Schedule 6, proposed Section 32F of Audit Commission Act 1998
[30] HL Deb, 7 Mar 07, Col 732
[31] Schedule 6, para 2, proposed section 32A of the Audit Commission Act 1998

conducted.[32] It provides a non-exhaustive list of additional purposes, including the prevention and detection of crime, the apprehension and prosecution of offenders and the recovery of debts owed to public authorities.

30. Data mining may help to detect fraud and may also have benefits in relation to these other purposes. Nevertheless, as discussed above, it is far from clear that these are sufficient to justify the sweeping invasions of privacy which indiscriminate data sharing and data mining inevitably involve. Given these serious privacy implications we consider it to be important that Parliament retains strong powers to control the purposes for which data mining may be conducted.

31. The Bill currently provides that any order to extend the purposes for which data mining may be conducted would have to be approved by a resolution of both Houses of Parliament.[33] We do not consider this to be sufficient in this context due to the limited time which is normally allowed to debate draft orders and, in particular, because Parliament would not be able to amend such an order. The Government could, for example, propose that the following extra purposes were added: (1) detection of serious crime; (2) preventing terrorism; and (3) identifying people who might be interested in taking part in a "Number 10 Policy Forum". Parliament may agree that purposes (1) and (2) justify the invasion of privacy that data mining entails but that (3) does not. It would not, however, be able to delete (3) and would have to vote for all or nothing.

Jago Russell, Liberty

[32] Schedule 6, para 2, proposed section 32G of the Audit Commission Act 1998

[33] Schedule 6, para 2