NO2ID Parliamentary Briefing on the Serious Crime Bill

Prepared by Guy Herbert, NO2ID General Secretary - 3rd – 7th February 2007

1. Legislative Context

NO2ID is concerned that the Serious Crime Bill ("the Bill", in what follows) contains some highly controversial proposals in Parts 1 and 2 and that these will "soak off" parliamentary attention from Part 3 – which is also extremely radical, but in an low-key technical way. "Data matching" is central rather than peripheral: this Bill creates the scope for endless secret 'fishing expeditions'.

This is a broad data-sharing bill

It is important to note that the data-sharing powers created in this Bill, like the radical alteration of incitement in Part 2, are not in any way confined to the new category of "serious crime", somewhat arbitrary and extensible though that category may be. The Bill's title is misleading.

The notional function of some of the Part 3 powers is largely "prevention" of crime, specifically fraud – though, as explained below, there is scope for them to be extended much more widely – and those added in cl.65 are for investigations that may be speculative. **It is not unfair to characterise these provisions as spying on the general public in case the information might be useful.**

In common with other data-sharing powers recently brought forward by the government, there is an attempt to vitiate data protection, rights to private life and common law confidentiality by legislative slight-of-hand. Some of the regulatory powers granted make a mockery of *ultra vires* and parliamentary oversight. This is consistent with the Government's Information Sharing Vision Statement, if not with the rule of law.

1.2 It is also a data-mining bill

"Data matching" is not a term unknown to law. It is however a term whose meaning is not well understood, and which is extended by this Bill, to make it **a high-tech version of the 'general search warrant' that has long been held to be repugnant to English law**. Such a warrant is effectively exercised in secret, because the persons whose information is rifled will have no knowledge that it is occurring. And the Bill contains provisions for personal information, including "sensitive personal information" under the Data Protection Act definition, to be passed to third parties to be defined in regulation, so that such a "warrant" need not be exercised by UK public bodies, but could be in private hands, or in the hands of overseas governments.

Throughout the Bill (to repeat what we have said in other briefings), in common with most recent legislation, there are **extensive provisions for compiling official database dossiers on individuals, and businesses through interrogatories and data-sharing**. While any form of investigation requires information, the cross-referencing and sharing of information (including some that would otherwise be absolutely confidential) for fishing expeditions, rather than following specific suspicions of a crime.

"Data matching" is what is known commercially as data-mining. It takes existing information in large quantities and makes new databases out of it, by mass cross referencing.

It is important to understand that this is not the same as tracing information on an individual pre-identified case through multiple sources of information. It means picking out individuals for suspicion based on relationships found in large masses of data.

Data mining is not generally disadvantageous to the subject in commercial customer service contexts. If Tesco suspects you might like tinned salmon, because people with similar shopping habits to you often do, and insists on sending you money-off vouchers, or Amex wants to offer you money off a ludicrously expensive golf-club membership, then you don't suffer noticeably.

However, the example of a government data-matching power we are all familiar with is less encouraging. TV Licensing regards not having a TV license as inherently suspicious. It therefore aggressively pursues anyone who is on the electoral register or other databases to which it has access who does not also match a household with a license on its own database. That principle is what the Bill intends to extend to full criminal investigations of all potential crime, and – ominously – through some subtle drafting to the pursuit of other government purposes too. Such investigations will be driven by much more complex assumptions about what might constitute a "suspicious" constellation of characteristics or behaviours.

That is the final point about data-mining. It is not a magical information tool. Like an oracle it requires interpretation, and is susceptible to showing patterns where the investigator expects to see them. Patterns are not necessarily meaningful; large quantities of data will throw up many relationships that appear to be meaningful by chance, and social network effects will add to this, creating the illusion of relationship and chains of relationship without meaning. (And they will miss other relationships that happen not to be captured by the data available, of course.) This is the well-known, and much-studied, but not well-understood "Small World" or "Six Degrees of Separation" effect. While Small Worlds and mistaken market segmentation do not matter in selling people grapefruit, when it comes to fabricating a presumption of guilt and/or applying the power of the state in individual lives, they matter a great deal.

The database state element of Government vision, which as "Transformational Government" forms **part of the broader motivation of the ID Scheme assumes that numbering citizens makes it easier to share and mine information about them**. The intended consequence of that vision is a Governmental all-seeing eye, with ever increasing scope for intervention in individual lives. If data mining is the means to pick individuals out for intervention it will impose official presuppositions on arbitrary sets of people - many of whom, in the context of this Bill, may end up labelled as "criminal associates": Guilt by association without even the association being real.

Data matching is also in detail open to the same concerns as any other data-sharing practice, these we discuss in relation to Part 3 powers.

2. Practical Consequences

2.1 Fundamental damage to presumption of innocence and protection of the innocent from criminal investigation

Data mining exercises presume there is something to be found. They pick out individuals as objects of interest on the basis of criteria containing presumptions about patterns of behaviour made by investigators. Unless it gives direct evidence of wrongdoing, this is an inherently prejudicial process leading to a search for confirmation of prosecutorial models: virtual crime.

Data sharing for financial purposes can cause financial detriment to individuals outside their control and which can be impossible to compensate. This is particularly true where Money Laundering Regulations result in loss of services without explanation, on the basis of suspicion.

2.2 Dangerous interactions of powers within the Bill and in other legislation

The Bill contains measures (SCPOs) that can in effect punish people for patterns of behaviour without any need for the commission of a crime by anyone. That gives scope for the prosecutorial models of behaviour alluded to above to result in actual punishment for individuals on the basis of "behaviour" that is an artefact of data-mining. The data-mining powers are not just applicable to crime, but to any government function and can result in analogous injustices in any sphere of government action with consequences for the individual – particularly where there is official discretion or decisions made on the balance of probabilities: a priori probabilities are very difficult to judge in many-dimensional data-spaces. The possibility of datamining will encourage its use on many official databases with scope for propagating and multiplying the errors and corruption in them. In particular the apparent 'foolproofness' of reference numbers from the National Identity Scheme will enable this. That is, the process, only, will be enabled. Paradoxically, increased confidence in information is likely to degrade its reliability: longer chains of inference will have more weak links.

2.2 Effective abolition of data protection in respect of financial information – increased fraud

The more data is shared, the more it can be misused. In the case of financial data, this is not just a threat to privacy but a direct invitation to fraud. The Bill provides for entirely arbitrary data-sharing with an entirely arbitrary class of persons designated by the Secretary of State, who may do with the information what they see fit. Not a recipe for privacy or security.

2.3 Effective abolition of data protection in respect of official use of data

The data-mining provisions incidentally give the Audit Commission, in its new role of government data-warehouse, carte blanche to handle and process personal information, including sensitive personal information, for official purposes.

2.4 "Small World" effects will mean arbitrary suspicion and pursuit of individuals, undermining both civil liberty and respect for law.

The sort of operations contemplated by the Bill involve very large and often unreliable data sets into which all sorts of patterns may be read. The likelihood of individuals matching a "suspicious" pattern by chance is very high. The sense that the authorities act capriciously or randomly – which reliance on data-matching as a tool of population management would ensure they did – would is corrosive of the values of a free society.

2.5 Building haystacks to look for needles: data-mining will waste resources not save them

Commercial datamining has external measures of success. Either it is profitable or it is not, and the profitability of particular actions can be monitored. This works well because it is aggregrative: the customer provides the feedback by participation or not at his choice, and a statistical success is a financial success. It is a compass.

Delivery (as opposed to management) of state services and regulatory and criminal enforcement is disaggregatory and must be enforced on the individual (which changes the balance of cost). Unless arbitrary punishment by computer is being suggested, statistical success is not acceptable justice must be done in the individual case as far as possible. Each case pinpointed by the database state must be separately examined. So since it necessarily multiplies cases it multiplies costs: there isn't as in a commercial transaction, a readily measurable return that limits the pursuit of particular lines of enquiry.

3. Specific points of concern

Part 1

Though Part 1 is principally concerned with matters outside NO2ID's purview we would draw your attention to the fact that nothing prevents an SCPO requiring the disclosure not just of information related to an individual the subject of an order but of broad categories of information about others that is in his control, which might be used for data-matching under other parts of the legislation.

Only banking and personal and journalistic confidential information appears to enjoy any immunity from such disclosure, under cl.13 – but the protection for banking information, at least, is more apparent than real, since consent under 13(3) may not be freely given but made a condition of any relationship by a banker who anticipates an order, and 13(4) overturns the protection whenever required (compare the circularity in cl.61(4) and cl.64).

The restrictions of cl.15 only protect the person who is forced to divulge information under threat of punishment using an SCPO from being prosecuted using it. So they do not prevent SCPOs being used to compel disclosure of information that is then used either to prosecute third parties directly, to provide leverage for further SCPOs, or - germane our concern about the database state - to facilitate "fishing expeditions" using data-matching powers. That data-matched information is obtained via SCPO is liable to condition the interpretation of subsequent data-mining in a prejudicial way, we suggest.

Part 3 – Chapter 1

cl.61-64 These sections create an entirely arbitrary regime for financial data-sharing in the name of preventing fraud. A "specified anti-fraud organisation" (SAFO) can be anyone the Secretary of State sees fit, and there is no provision for oversight of their continuing fitness. There is no provision for a general code or regulation of the sharing, it is a matter for individual arrangements. Only SAFOs themselves are subject to specification by regulation.

61(2)(b) seems to suggest that if there is a SAFO involved in the process, then disclosure can be to anyone at all.

61(3) casually sets aside common law confidentiality, and *ultra vires,* and any statutory restrictions.

61(4) looks like a safeguard, but isn't. It is presumably there so ministers can point it out to incurious Government backbenchers as guaranteeing the Data Protection Act applies. This is worthless because under cl.64 the Data Protection Act is amended to make almost anything that might be done under the rubric of ccl.61-63 fall within its terms.

62 contains some protections in relation to certain classes of information, but they are extremely limited, and the offences concerned are really only in existence to punish (they can't prevent) misconduct by individuals. In the light of other clauses, one cannot see how an organisation, private or public, would be inhibited from disclosing information by these provisions.

63 is also interesting as limiting safeguards. Prosecutions for abuse of information-sharing are controlled by those bodies who will be using the procedures. There's no suggestion that the Information Commissioner might be involved.

cl.65 – makes very significant amendments to the Audit Commission Act 1998 via the insertion of the eight sections contained in Schedule 6. The Government is seeking broad powers which could permit the use of sensitive personal data in data matching exercises involving both the public and private sector that can be extended to any government purpose by regulation. Not just crime, let alone "serious crime".

For now, data matching under the Audit Commission Act 1998 restricts the process to specific uses of data (for example, the comparison of lists of Local Authority employees with lists of state benefit claimants in order to identify potential benefit fraud).

These new powers in Schedule 6 extend the data matching remit of the Audit Commission so it can perform data matching in the context of "assisting in the prevention and detection of fraud" and possibly other purposes such as "debt recovery". Given that the Audit Commission's remit is usually concerned with the efficient and effective delivery of public services, the powers in the Bill are so broadly drafted they have the potential to legitimise data matching for the purpose of identifying individuals who are being served in particular ways by NHS Trusts or Local Authority services. This would be in line with the government's ambitions for the "personalisation" government services, and interestingly parallels one part of the definition of "necessary in the public interest" for the use of national identity scheme data under the Identity Cards Act 2006.)

Under the data matching provisions, the Audit Commission can obtain "such data as the Commission may reasonably be require for the purpose of conducting data matching exercises" from many public bodies and cross match these data with data held by certain other bodies – those public bodies which are already obliged to give the Audit Commission personal data and other bodies (public and possibly private) which can volunteer to provide personal data, whether or not the data was obtained voluntarily.

The bodies which are subject to mandatory data collections are those currently fully subject to the Audit Commission's audit powers, e.g. police forces, emergency services, local authorities and NHS Trusts – but not government departments.

There are no limits on type of personal data requested for data matching exercises, thus such exercises could even include "sensitive personal data", for example medical or criminal records. Where the Commission performs additional data matching exercises for

any other body, then these data matching exercises cannot include "patient data" relating "to an individual which are held for a medical purpose". This exception implies that medical records can be used where data matching involves a body where there is mandatory disclosure to the Audit Commission. Further the prohibition only applies to medical records; it follows that any other form of confidential or sensitive personal data (e.g. criminal records) could be used in any other form of data matching exercises (e.g. the use of criminal records to compare trends in one Police Force with another).

The Secretary of State is also seeking powers to extend data matching to other bodies and for purpose which extend beyond those related to crime. For example, the Bill identifies the purpose of "to assist in the recovery of debt" as a likely area where data matching techniques could be used by the Commission but, under the Bill, the Home Secretary or other Secretary of State "may by order add further purposes for which data matching exercises may be conducted". The power allows the Secretary of State to add to the "public bodies" which could fall within the category which are obliged to provide personal data to the Audit Commission for data matching. Note that the use of the term "public bodies" in this provision carries the implication that the use of the words "body or person" not qualified by the word "public", elsewhere in the Schedule, is intended to include the private sector.

The Bill does not contain detailed measures to protect the interests of data subjects – or classes of individuals – in data matching exercises and the presumption is that any safeguard is to be contained in a Code of Practice to cover all "data matching exercises". This Code is to be drafted by the Audit Commission and unlike, say PACE Codes of Practice, the Audit Commission's Code is not to be laid before Parliament. The only (potential) material protections for privacy and against the prejudicial conduct of data-mining will not be subject to Parliamentary approval. The Bill also states that the Commission will be under an obligation to consult public bodies (e.g. NHS Trusts, Local Authorities) as to the content of the Code but there is no explicit requirement to consult the Information Commissioner, nor those whose data might be subject to mining.

The Code of Practice is important. Can a single Code of Practice cover the whole range of purposes associated with data matching? What are the triggers which justify the decision to embark on a data matching exercise and how will these be communicated to the public or even data subjects? Will the Commission publish the assumptions made in the matching program and how will the Commission measure or publish the outcomes and who audits the auditor's assumptions prior to a matching exercise? How will the Commission show that data matching is a proportionate use of powers, particularly since it is presumed to act on behalf of other public authorities in such matters rather than on its own initiative? Will it refuse requests? Can it?

If the Information Commissioner has no control over the content of the Code, what reports will he (or parliament) receive about each data matching exercise, or such procedures in general? What is the mechanism which prevents excessive use of powers? These are serious questions one hopes that Ministers will NOT deflect such awkward procedural questions with the comment: "don't worry - these will be in the Code of Practice".