We are right to fear spy 'database of everything' if even politicians know little about it

March 18 2015, by Eerke Boiten

(Security) Service with a smile. Credit: rogersg, CC BY-SA

The recently released Intelligence Service Committee's report suggested an overhaul of the laws governing the work of the intelligence and

security agencies. But beyond the headline announcement were buried details and admissions to questions that have gone unanswered for more than 40 years.

To find out why we must go back to 1972 when, as computerisation continued apace, concerns about the role of "data banks" grew into fears of large, centralised and intrusive databases containing details of everybody's lives. In response the government set up the Younger Committee, which introduced ten principles to guide the growing use of computers for the processing of personal data.

When the government finally responded to the Younger report in 1975, it agreed that "government and private data banks should be considered and controlled together". It also insisted that different data banks should not be linked unless "expressly sanctioned by law or agreement, or are subject to scrutiny and control" by the same authority.

These recommendations and the ten principles went on to underpin data protection law, from the first Data Protection Act in 1984 until today. This covers both private and public sectors, though there are exceptions for areas such as national security in this and those laws that succeeded it.

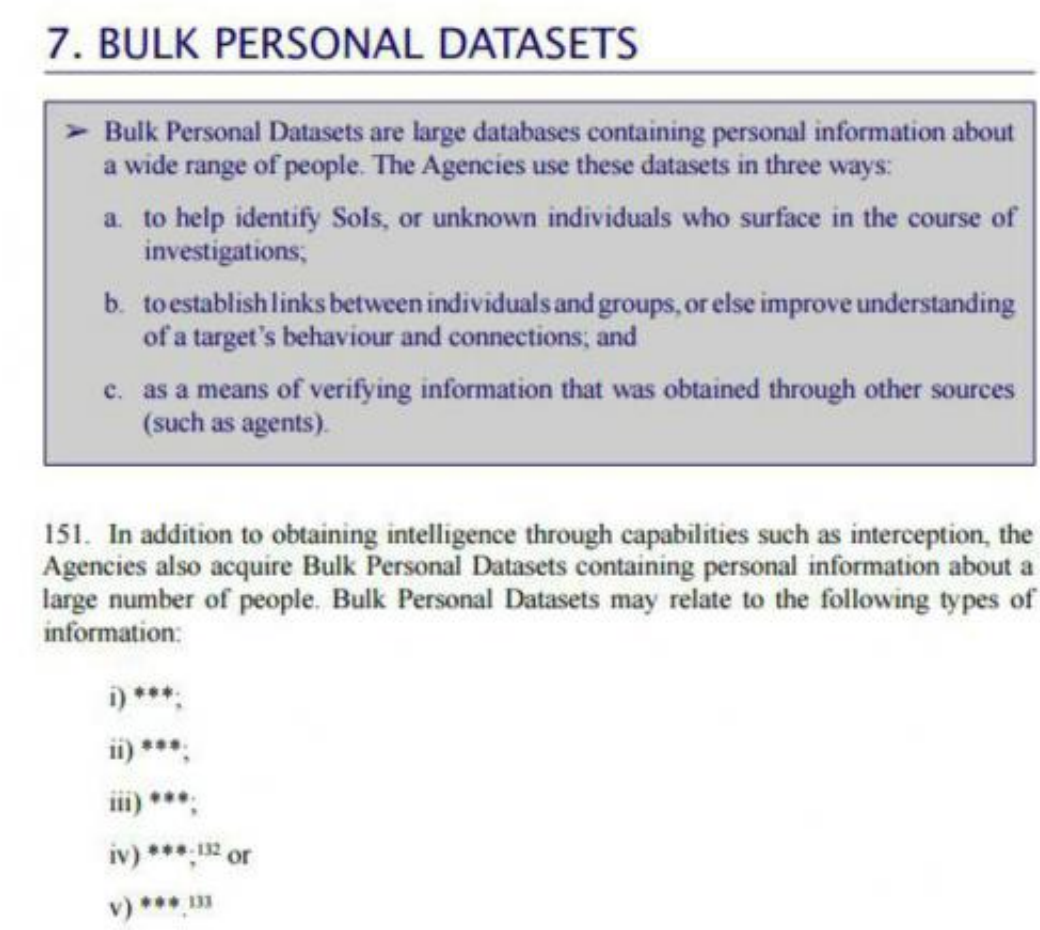
Fast forward to February 10, 2011 when, after almost a decade of heated debate about a UK national identity card, the hard disks that contained the partial implementation of the National Identity Register database that underpinned the identity card scheme were physically destroyed.

It's tempting to view the next similar hardware destruction, that of The Guardian newspaper's computers containing Edward Snowden's leaked files in July 2013, as a somehow ironic remark by GCHQ on the previous.

It was obvious to anyone that copies of the files remained elsewhere at The Guardian and the other media outlets involved in the scoop. The chain of events set off by Snowden's revelations must now make us wonder whether GCHQ still holds a copy of that National Identity Register – and much more besides.

A database of everything

This issue raises its head in this report of the Intelligence and Security Committee, the UK parliamentary committee that oversees the work of MI5, MI6 and GCHQ. In response to the news stories based on Snowden's leaked information in 2013, the ISC first stated that GCHQ had not circumvented or attempted to circumvent UK law – a claim received with cynicism by parts of the press, but barely challenged by politicians with the exception of the Home Affairs Committee – and subsequently launched an inquiry.



7. BULK PERSONAL DATASETS

➢ Bulk Personal Datasets are large databases containing personal information about a wide range of people. The Agencies use these datasets in three ways:

a. to help identify SoIs, or unknown individuals who surface in the course of investigations;

b. to establish links between individuals and groups, or else improve understanding of a target's behaviour and connections; and

c. as a means of verifying information that was obtained through other sources (such as agents).

151. In addition to obtaining intelligence through capabilities such as interception, the Agencies also acquire Bulk Personal Datasets containing personal information about a large number of people. Bulk Personal Datasets may relate to the following types of information:

i) ***;

ii) ***;

iii) ***;

iv) ***;[132] or

v) ***.[133]

Not particularly enlightening.

That inquiry's final report reveals that the "database of everything" first feared in the 1970s had existed all along, in the form of Bulk Personal Datasets (BPDs) held by the intelligence agencies. Acknowledged for the first time, this strains the ISC's earlier claims of adequate knowledge and oversight and no practices that stretch or break the law.

BPDs are defined in the report as "large databases containing personal information about a wide range of people", some with millions of records. What kind of information this might be appears to have been entirely redacted. They are acquired "through overt and covert

channels", linked to other datasets where needed, and shared at will between the agencies and also with overseas partners.

For every past, current and future personal database (perhaps care.data?), we should now worry whether it is linked into this database of everything accessible to the security services not just in the UK, but perhaps other allied countries with very different views on data protection.

No insight, no oversight

The ISC is rightly concerned that "legislation does not set out any restrictions on the acquisition, sharing and destruction of Bulk Personal Datasets, and no legal penalties exist for misuse of this information". There is almost no oversight in how they are created and used – even the home secretary and foreign secretary do not get involved beyond general discussions about BPDs. Instead, the agencies work with them on the basis of the Intelligence Services Act 1994 and Security Service Act 1989, and take unsupervised decisions on the basis of Human Rights Act's principles of "lawful purpose, necessary and proportionate".

The information security commissioner, Sir Mark Waller, does include BPDs in his review visits, though not on a statutory basis, nor with any mention in the publicly accessible part of his report. That the only immediate response to the ISC report from the prime minister, David Cameron, was to make BPD oversight a statutory task may be viewed as an indication that BPDs are seen as important.

In his recent book Black Box Society Frank Pasquale, professor of law at the University of Maryland, describes how so-called Fusion centres were established in the US after 9/11 to support the intelligence agencies and their industrial partners. These were US equivalents of this "database of everything", where public and private data of all kinds – tax, health,

traffic tickets, utility bills, insurance – were combined and sifted. Such databases would inevitably also include information about UK residents, and so it's likely Fusion centre databases would also be part of any sharing arrangement with UK agencies' BPDs.

Data retention

The ISC report mentions many datasets throughout, such as those that include the "bulk collection" of "communications data", or even the contents of private emails, texts and calls. In each case, the retention period is redacted. This lack of information should pose difficult questions for the agencies, considering retaining this sort of insufficiently targeted surveillance data was ruled unlawful by the Court of Justice of the European Union in 2014. Although it seems that by simply copying data into unregulated BPDs the agencies can retain the data indefinitely.

Going back to the original "data bank" fears, the usual questions reappear: what happens if BPD data is incorrect? What if incorrect data leads to action against citizens? Due to the National Security exemptions on data protection, there is no right to access, no right to correction and no right to redress. How are we to know if the data is secure and how would we find out if it gets abused by an insider – an eventuality that the report admits has already happened – or hacked from outside?

The database of everything feared in 1972 when computer processing power was exponentially smaller than today has finally come to light in 2015, at a time when far more data and data from far wider sources can be included. If even the government itself has only a tenuous grasp on the fact this mechanism exists, let alone a thorough oversight of it, we are right to be concerned.

Commons-Attribution/No derivatives).

Source: The Conversation