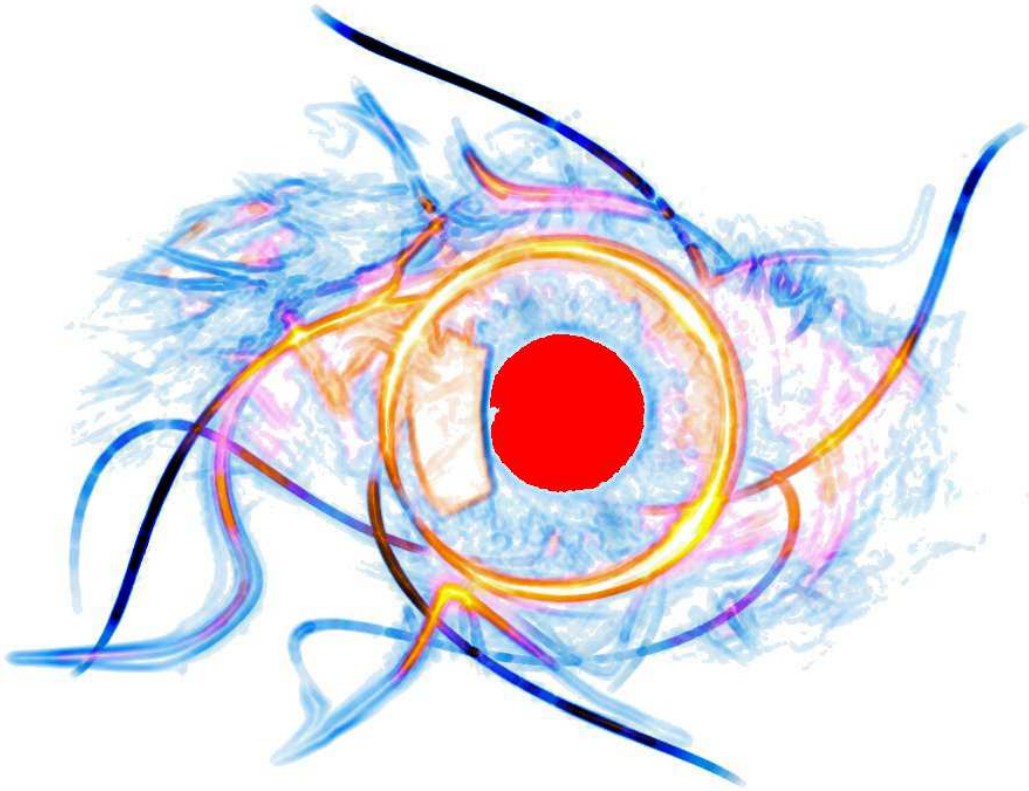
Paper on a Single Resident Record for the Isle of Man



"The United Kingdom has never had a secret police or internal intelligence agency comparable to those that have existed in some other European countries... There has however been growing concern in recent times about surveillance and the collection and use of personal data by the state...

...such concern on this side of the Channel might be said to have arisen later, and to be less acutely felt, than in many other European countries, where for reasons of history there has been a more vigilant attitude towards state surveillance...

The higher level of concern elsewhere in Europe is reflected in the repeated condemnation by the European court of the law of this country in this area, often on the basis that the law contains no adequate safeguards..."

Lord Reed, Justice of the Supreme Court of the United Kingdom, in T & Anor, R (on the application of) v Secretary of State for the Home Department & Anor [2014] UKSC 35 (18 June 2014)

Introduction

1. Proposals have been put forward for a Single Resident Record for the Isle of Man. This paper reviews some of the issues arising, for the purposes of informing the consultation and debates about the proposals. In particular, this paper focuses upon the risks and dangers that are associated with a Single Resident Record. That is not because there are no potential advantages or benefits. Rather, it is because advantages and benefits will be put forward by those proposing the database in any event; it is the disadvantages and dangers that run the risk of being overlooked.

2. More specifically, I have been briefed to address "*what would need to happen for the Single Resident Record to be Article 8 compliant [taking] in recent case law and ECJ judgments as well as the GDPR*." The reference to Article 8 is a reference to compliance with human rights law, and is addressed below under the heading 'Databases and The Human Right to Privacy'. The reference to the GDPR is a reference to the General Data Protection Regulation, a recent EU Regulation that is being implemented, and is addressed below under the heading 'Current and Future Data Protection Law'.

3. In opening, I analyse the concept of a Single Resident Record. I then frame the database in the context of current and future data protection law and of human rights law, and finally use that framing to inform the discussion of particular issues.

What is a Single Resident Record?

4. The concept behind a Single Resident Record is that the information held by government about individuals is consolidated into a single database, maintained in electronic format.

5. Various branches of government will have maintained databases that will have evolved over time, for their own purposes. A Single Resident Record envisages that in future, separate databases will become redundant.

6. Conceptually, however, there is no bright-line distinction between what is, and is not a single consolidated database:

   - Consolidation can be achieved by ensuring that individual databases can communicate effectively with each other; or that they communicate effectively with a new centralised core; or that they are totally replaced by a new system;

- ❖ Information held on such a database can be garnered by merging it from existing information already held (with the consequent risk of replicating any errors or conflicts along the way); or by transitioning over time so that new and old systems run in concert (with consequent complexity, and loss of the perceived benefits of tidiness and efficiency); or by manually populating a new database (reducing the risk of errors and conflicts, depending on how it is done, but a huge investment in human resources for what is intended to be an electronic database).

7. Just as it is possible to create a database in a variety of different ways, so equally it is possible to limit access to that database in a variety of different ways. One of the concerns expressed about a single consolidated database, further explored below, is the enhanced risk of information being inappropriately shared, hacked, lost or stolen.

8. Protagonists who favour a Single Resident Record are likely to argue that these risks will be addressed by careful safeguards that limit access to and sharing of information on a need-to-know basis, with transparent rules about who is allowed to access what, and when, and with what level of security.

9. What is often missed in such arguments is that these internal hurdles to limit the sharing and transfer of information are effectively recreating the existing limits and constraints that arise from multiple fragmented databases. Any reconstruction of internal barriers to the transfer of information might reassure the doubters, but also raises inherent questions about the benefits: most of the perceived benefits depend upon the ease with which information can be transferred and analysed; protections against misuse require making it harder to transfer and analyse information.

10. I suggested that a Single Resident Record was conceptually about information held by ***government***. Certainly in England, an astonishing array of what were once public services delivered by government are now routinely delivered by commercial and third sector bodies under contract with government. This includes health services, child protection and social care services, the administration of social security benefits, the management of prisons and immigration detention centres, and defence services.

11. In considering the risks and disadvantages of a Single Resident Record, it is necessary to consider how information might be input or extracted by commercial entities

(and how it might be hacked, lost or stolen from commercial entities) as well as government. Even if there is little involvement of commercial entities now, consideration would need to be given to possible future involvement over the lifetime of a Single Resident Record scheme - year and maybe decades hence. In considering commercial entities, it is also necessary to reflect that, again conceptually, it is possible to merge information that individuals have shared with commercial entities (generally ***with consent***) with information held by government (often ***without consent***, see the discussion on consent below).

12. Commercial entities might also have their own interest in the use of government data, not only for targeting sales or achieving government-imposed targets, but also as a proxy for actuarial assessment (accurately assessing risk and probability, influencing the cost of services such as the provision of pensions or insurance).

Current and Future Data Protection Law

13. Current data protection law is broadly framed to meet European Union legal standards, primarily but not exclusively EU Directive 95/46/EC. The nature of data recording, storage, transfer etc has changed beyond all recognition in the last two decades, and the European Union has undertaken a fundamental review leading to a new Regulation, colloquially known as the General Data Protection Regulation (EU) 2016/679, shortened to the "GDPR".

14. Domestic legislation is needed to implement the GDPR by May 2018, when the GDPR will replace the current Directive and will be directly applicable in all Member States. Of course, that date falls during the two years after the United Kingdom triggered Article 50 signalling its intention to leave the European Union.

15. In theory, data protection law might be caught up in the fractious and contentious arguments about the relationship between the United Kingdom and the European Union (and in the Isle Of Man, the tripartite relationship whereby the Island's relationship with the European Union "hangs on the coattails" of the United Kingdom's relationship with the Union.)

16. In practice, however, data protection law is not currently contentious in this way. In simple terms, this is because if the United Kingdom – and the Isle Of Man – wish to trade with the European Union, then they must have in place a data protection regime that corresponds at least "adequately" to the GDPR. The United Kingdom has recently (14th September 2017) published its Data Protection Bill, intending to deal

with both of the requirements of the GDPR and departure from the Union. Driven by the need for trade with the Union, the approach of the Bill is broadly to implement the GDPR, and to preserve that implementation after any departure from the Union.

17. It is noteworthy that the proposals on the Isle Of Man for a Single Resident Record arise at the same time as the Island would be required in any event to review its data protection laws for compliance with the GDPR. For the purposes of this paper, I am going to assume that compliance on the Island with the GDPR is uncontroversial as it is in the UK.

18. However, it does not follow that a Single Resident Record is uncontroversial. Not only is such a database not required by the GDPR, but there are requirements of the GDPR that might lead to real questions about such a database.

19. It is worth noting also that in at least one area relevant to any centralised government database, the UK is at odds with the European Union. This relates in particular to the collection and retention of information about the private electronic communications of citizens.

20. In Digital Rights Ireland (Judgment of the Court) [2014] EUECJ C-293/12 (8 April 2014), the European Court of Justice ruled that this breached citizens' privacy rights. The United Kingdom responded, effectively in defiance of the Court's ruling, by passing legislation to authorise what has been ruled unlawful (the Data Retention and Investigatory Powers Act 2014). The lawfulness of this act of the United Kingdom's Parliament was challenged in a case brought jointly to the European Court of Justice by Labour deputy leader Tom Watson and, ironically, Conservative David Davis who is now the Brexit Secretary. Unsurprisingly the Court ruled against the United Kingdom (see Tele2 Sverige (Judgment) [2016] EUECJ C-203/15 (21 December 2016)). The European Court ruled that this legislation was in breach of European law. The legislature had moved on, however, supplanting that law with the Investigatory Powers Act 2016. Permission has been granted to Liberty to further challenge the lawfulness of the new regime. As their press release of 30th June 2017 notes,

> The High Court has also allowed Liberty to seek permission to challenge three other parts of the Act once the Government publishes further codes of practice, or by March 2018 at the latest. These cover:
>
> - Bulk and 'thematic' hacking – the Act lets police and agencies covertly access, control and alter electronic devices like computers, phones and tablets on an industrial scale, regardless of whether their owners are suspected of involvement in crime – leaving them vulnerable to further attack by hackers.
> - Bulk interception and acquisition of communications content – the Act lets the State read texts, online instant messages and emails, and listen in on calls en masse, without requiring suspicion of criminal activity.
> - Bulk personal datasets – the Act lets agencies acquire and link vast databases held by the public or private sector. These contain details on religion, ethnic origin, sexuality, political leanings and health problems, potentially on the entire population – and are ripe for abuse and discrimination.

21. Given the history of this litigation, it can be said with a high degree of confidence that the United Kingdom's giving itself broad powers to hold and use databases, to retain data, and to do so without needing to show good cause or affording review, **is and will continue to be found to be unlawful**. I have described this as "one area relevant to any centralised government database". At this very preliminary stage, this paper is highlighting risks based upon what is technologically possible. It has to be observed that to the extent that government is able to see private communications, it is also able to link information to any other information it may hold in its databases. This was a specific concern expressed by the Court in the Watson and Davis case:

> "That data taken as a whole is liable to allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as everyday habits, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them…In particular that data provides the means…of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications" [Tele2 Sverige (Judgment) [2016] EUECJ C-203/15 (21 December 2016) at paragraph 99]

22. It should be borne in mind that even where there may be a difference between what is technologically possible and what is legally possible, what is legally possible would not constrain those who wish to hack or otherwise misuse database information.

Data Protection Law and Consent

23. Under current data protection law, data processing is widely a broadly defined to include viewing and accessing data, using it, manipulating it, deleting it, but perhaps most controversially, sharing it. Data-processing has to be fair and lawful, and also fall within the framework that sets out the purposes for which data can be processed.

24. Data can be processed – and therefore information can be shared – with informed consent. It can also be shared without consent in a number of circumstances, many of which would apply to government. These give rise to what are often termed "statutory gateways" – where a piece of legislation which authorises or requires information sharing also effectively provides the basis for doing so without consent.

25. The relationship between statutory gateways and the seeking of consent is highly controversial. One reason is that it has been argued (for example in relation to the controversial Scottish scheme to impose a "named person" with oversight of the well-being of every child) that if information is going to be shared without consent, consent should not be sought.

26. For my part, I believe that argument is wrong. I believe that it is good practice – good ethical and professional practice, likely to enhance trust – to try to work with consent wherever it is possible.

27. The Supreme Court of the United Kingdom, in a judgment overturning the Scottish legislation, identified and expressed concern about one of the probable consequences of routinely operating without consent: it is a fundamental right to have access to a remedy for misuse of data by the government. Exercising that fundamental right requires that you have some way of knowing what the government is doing with your data, and if government routinely processes it without your consent, you will have no idea whether they are using it lawfully or not.

28. The new GDPR addresses this issue around consent in statutory gateways. It says this:

> 42. ...Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.

> 43. In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.
>
> [GDPR, recitals]

29. On the face of it, that part of recital 42 reproduced above might seem to legitimate a stance that consent should not be sought if the State is going to process your information anyway. That is a dangerous reading of the recital, likely to lead to two further possible errors. ***Firstly***, the erroneous belief that if consent is not needed, then transparency is not needed either, because the processing is going to take place anyway. ***Secondly***, the erroneous belief that processing of information must be lawful somehow in some other way. Read as a whole, the true position is that there might be no alternative to seeking consent in circumstances where a measure is not necessary or proportionate; so the GDPR is actually saying that if the State is going to process information in unnecessary ways, it had better mind itself to go out of its way to make sure that consent is fully informed, freely given, not subject to any detriments, easily withdrawn, not misused etc.

30. In other words, the GDPR enhances the rights of the ordinary individual not to have their information processed without consent, and in particular, diminishes the right of government to argue that consent is not needed because the processing has been made lawful by some other means.

31. This is highly pertinent to the issue of the Single Resident Record. If such a database is going to comply with the spirit of the GDPR, ordinary individuals ought to know who is accessing the information, when, and how, in order to form their own view on whether it is lawful, and hold the government to account if necessary.

Databases and The Human Right to Privacy

32. The European Union uses the language of "fundamental rights". One of these declared fundamental rights is "*Everyone has the right to the protection of personal data concerning him or her*". The data protection laws discussed under the previous two headings refer back to this fundamental right.

33. However, human rights are universal. They do not refer back to European Union law. The European Convention on Human Rights and European Court of Human Rights are not European Union institutions. I am now discussing these human rights, which do not refer back to European Union law, and will be unaffected by any changes in the relationship between the Isle Of Man, the United Kingdom, and the European Union.

34. In human rights terms, the protection of personal data is an aspect of Article 8, the right to respect for private and family life.

35. In 2002, an 11-year-old boy, now known only as T, received police warnings in respect of the theft of two bicycles. 8 years later as an adult, he applied for enrolment on a sports studies course, which was to entail his contact with children. The result and checks revealed his bicycle thefts as an 11-year-old, and threatened his place on the course, leading to litigation which went all the way to the United Kingdom's Supreme Court.

36. The quotation on the front cover of this paper is taken from the judgment of the Supreme Court in that case. It explains how those who have not experienced the misuse of data and state surveillance can sometimes overlook the real risks and dangers that are there. This is sometimes expressed in the aphorism "if you have nothing to hide, you have nothing to fear". This statement is false. It's truth would rely upon at least two huge leaps of trust: ***firstly***, that at no point in the future will the government authorise any adverse consequences for the decisions that you have made today; ***secondly***, that you trust that no third party will misuse the information that you have not hidden (for example, to enter your bank account, burgle your house while you are out of it, hike your insurance premiums, or infect your computer with ransomware...)

37. That Supreme Court case illustrates some of the risks:

- ❖ it illustrates how difficult it can be to know or foresee what the long term consequences of an unwise decision that is recorded might be. In particular, where someone suffers adverse consequences many years later in respect of something they did as a child, it illustrates the urgent need for a "right to be forgotten". (As the court observed, information is "*available for disclosure long after the event when everyone other than the person concerned is likely to have forgotten about it*", paragraph 106);

- ❖ it illustrates the need to foresee and address the possibility that information held and passed on by the State is used to the detriment of the individual by *somebody else* – in this instance, higher education institutions and employers. So do people understand that any consent they might give to being on a Single Resident Record might lead down the line to information being shared and used to their detriment by someone other than the Government to which that consent was given?

38. Importantly, the Supreme Court reviewed the case through the lens of human rights. The Isle of Man's Human Rights Act broadly mirrors that in the UK, and therefore the approach and outcome should also do so. The key right was, of course, the right to respect for private life. The judges were in agreement that the State can only interfere with this right both where it is in accordance with the law, and also where it is necessary and proportionate to do so. One of the judges explained how in his view it was unlawful because notwithstanding that there was an identifiable law, the law was capricious in its effect. The other explained how in his view it was unlawful because it was unnecessary.

39. For the purposes of considering a Single Resident Record, the agreement about the result lends the lie to the idea that passing a law to set up and maintain a Single Resident's Record provides all the necessary legal authority to do so. It is precisely because fundamental rights are engaged, that the passing of a law is only the beginning of the possible challenges, if the law is capricious in its effect, or the public authorities are negligent in its implementation.

40. It is worth observing that in this respect, concerns about a Single Resident Record may well mirror the UK mainland experience in relation to identity cards. Legislation was introduced by the then Labour government in the Identity Cards Act 2006 for an identity card scheme. The scheme got as far as a pilot, but was subject to a broad range of criticisms, most of them directed more towards the consequences of the underlying database that was inevitably behind the physical cards. These included:

- ❖ data protection concerns – the Information Commissioner memorably observing that "*my anxiety is that we don't sleepwalk into a surveillance society*";
- ❖ human rights concerns – the Westminster Parliament's Joint Committee on Human Rights raising concerns that the scheme was not compliant with Article 8;
- ❖ concerns about mission creep – the potential for significant expansion of the scope of the scheme being built into the legislation;
- ❖ concerns that the scheme would effectively become mandatory – for example upon renewal of driving licences;
- ❖ concerns that black and minority ethnic groups, and other vulnerable adults would be particularly vulnerable to misuse and abuse of the scheme;
- ❖ concerns that the scheme made identity theft easier, because a complete identity was tied up in a single database;
- ❖ concerns that the scheme was likely to be targeted by organised criminals;
- ❖ concerns that the scheme was not cost effective.

41. In the light of the wide-ranging concerns, the scheme was abandoned and the Identity Cards Act 2006 was repealed in 2010.

Database Security

42. Thus far, consideration has been given primarily to the risks associated with how the information held on a Single Resident Record is used by the government which has control of that database. However, a major concern is about the risks that are associated with its losing that control. This might be on a small scale (unauthorised access of an individual record), or an industrial scale (hacking of the complete database for download and sale on the dark web).

43. It could not properly be said that a Single Resident Record would not be of interest, or would not be at risk. Some examples of reported data breaches in simply in the last few weeks have included the following:

    - ❖ Equifax, which maintains credit reference services, last month revealed it had identified a data protection breach affecting more than 140 million customers, including in the UK. This breach would allow users in possession of the data to obtain further information by including the stolen information

as an "identifer" to (wrongly) reassure the recipient that communication was genuine and not a phishing exercise;

- Hackers may have infected more than 2 million computers with malware, by hacking into and using the legitimate download avenues of anti-virus software provider CCleaner.

- Earlier this month, the Estonian government identified a security risk in its ID cards, affecting more than half the country's population.

- And, of course, recordings forming part of child protection social work records were apparently stolen from an office on the Isle of Man earlier this year.

44. It is sometimes argued that a single consolidated database reduces the risk of security breaches. This is presumably on the basis that it is old technologies, and the mechanisms required to share information between old technologies, that pose the greatest security risk. This would appear to be an incomplete and misguided approach to security risk. The security measures taken to protect data or the transfer of data are only part of the equation; the value of the data, and therefore the value of hacking the data represents the other part of the equation, and the more integrated a database is, the greater the value of the hack. To put it another way, even if the security is greater, the likelihood of being targeted is greater also, and the examples of successful targeting indicates that an impenetrable whole system is unlikely.

Who Is the Record for?

45. I indicated in opening that the advantages to a consolidated database would doubtless be advanced. It is likely that the advantages advanced would include needing to provide information only once rather than to multiple different parts of government; and the ability to collate and use information for profiling and research purposes, for example in order to advance medical science or for comprehensive social research endeavours. It is worth taking careful note of whether or how those benefits actually accrue to individuals, or whether the government takes the benefit.

46. By way of example, it is well-established in the UK that the financial value of unclaimed and under-claimed benefits is many times greater than the value of fraudulently claimed benefits. Yet governments devote significant resources to

targeting fraudulent benefit claims and reducing them, without actively promoting the take-up of unclaimed and under-claimed benefits. The public seems to take for granted that benefit fraud is a problem to be addressed. A detailed and consolidated profile of the circumstances of the population is likely to be able to throw up information helpful to identify both fraud and unclaimed or under-claimed benefits. Would government use a record to facilitate the take-up of benefits? What about the use of health profile information in order to improve healthcare? What about the ability to identify employers and landlords who must be discriminating unlawfully – would the information be used to target organisational discrimination?

47. In considering the question "who is the record for?", it is worth revisiting the list of concerns and objections raised regarding the UK's Identity Cards Act, at Paragraph 40 above. It is striking that what lies behind those concerns is that there can be considerable benefits for the State in having a detailed profile of its population; and there can be a considerable benefit for commercial companies in having such information; and there can be considerable benefit for organised criminals having such information. I observed in opening that a Single Resident Record was likely to be promoted on the basis of its benefits to the citizen. While it may be convenient to the citizen not to have to repeat information to a range of different government departments, it is hard to see that such an all-encompassing scheme is being introduced in order to convey that benefit. The nature of the concerns suggests that the preponderance of the benefit is unlikely to accrue to the citizen. It is particularly concerning that this should be the case when the harm is likely to be irreversible: once the database is hacked, the information is "at large" and capable of being cloned multiple times, and cannot be put back into the box.

48. As explained in paragraph 90 of the "named persons" case in the UK Supreme Court, human rights law addresses this by requiring that interference with individual rights takes the least intrusive form possible. In that case, it was held that there was a "risk of disproportionate interferences", that was capable of being addressed by clear guidance, careful avoidance of unnecessary information sharing, and being clear about the role of consent and where there was a right to give or withhold it. Once again, this cuts both ways (compare paragraph 9 above): if a Single Resident Record is firmly grounded in true informed consent, and thereafter limited to the minimum necessary to achieve its public interest purposes, then it may be the least intrusive means and thereby compliant; but along the way, its benefits as a universal database held by the State will have been neutered.

Conclusion

49. I said in opening that I would highlight risks and disadvantages associated with a Single Resident Record. This paper is not able to scrutinise and evaluate any specific proposals, because I understand specific proposals are not available for such analysis. However, I consider, for two particular reasons, that that is not a limitation on what this paper can usefully set out. **Firstly**, it should be apparent that many of the risks arise from trying to future-proof proposals, in an era when the nature of what is possible is expanding so fast, and the ability to create and store new and more intrusive forms of evidence (such as CCTV and GPS location data) indefinitely is increasing at an exponential rate. ***Secondly***, it should be apparent that many of the risks are inherent in the unlawful use or misuse of data, rather than its use in accordance with any scheme which is devised and set out. Both of these issues can be addressed without knowing the details of a proposed statutory scheme. I hope this paper informs the debate accordingly.

Allan Norman September 2017