The Foundation for Information Policy Research

Consultation response on

The Data Sharing Review

Background

The Foundation for Information Policy Research (FIPR) is an independent body that studies the interaction between information technology and society. Its goal is to identify technical developments with significant social impact, commission and undertake research into public policy alternatives, and promote public understanding and dialogue between technologists and policy-makers in the UK and Europe.

We would like to make clear at the outset that we do not accept the apparent assumptions of this review. We do not agree that data sharing is simply a matter of utilitarian trade-offs, supervised by national governments. Privacy is founded in human rights – specifically in the European Convention on Human Rights, as refined in the Data Protection Directive and imported into UK law by the Human Rights Act. The Government of the day cannot extinguish these rights short of withdrawing from the ECHR, repealing the Human Rights Act, and quite possibly withdrawing from the European Union.

This review should be conducted in the framework of European law as it is, rather than on the basis of what some actors might wish that it were. Its subject matter must be seen in a European context – of our shared culture of values backed by constitutionally-embedded human rights, that include rights to privacy. Britain is going out on a limb by sharing data between public-sector databases far beyond the limits of what other European countries consider acceptable or even useful.

There are of course private-sector implications of data sharing. These range from the regulation of new technologies with privacy implications, such as Facebook, to the negative effects of the NHS National Programme for IT (NPfIT) on European markets for healthcare IT. But these are European issues too: Facebook will be regulated by the privacy and competition authorities in Brussels, and attempts to impose national autarky in public-sector procurement not only raise Single Market issues but will probably also fail in the medium term because of the pressures of globalisation.

In what follows we will therefore focus on public-sector information sharing.

What information sharing is lawful?

The consultation document invites respondents to write an extended essay on those aspects of data protection that concern them. FIPR has already written a substantial report on children's databases for the Information Commissioner in 2006, and we incorporate it in this response by reference[1].

In that report, we set out the legal position in detail. Sensitive information, such as that relating to health, sex life, religion, and political beliefs, may only be processed by consent or by means of specific statutory provisions. Member States may make laws overriding consent for certain clearly defined purposes like child protection, but not for general aspirational purposes like child welfare, improving public services or doing medical research. This is perfectly right and proper. Personal autonomy should not be overridden except on the basis of necessity: convenience is not good enough to justify it. Individuals should neither be compelled to consent to information sharing, nor discriminated against if they do not. Indeed, under European law, coerced consent is not valid, and compelling people to consent to information sharing serves no useful purpose (except perhaps to sensitise them to the fact that their rights are being infringed).

Unfortunately, the UK Government has for years ignored this law. Systems supporting healthcare, child welfare, research and other public policy objectives are being built that are not only unsafe but also illegal. We documented in great detail in our report how the databases being built, and linked up, to support children's healthcare, schooling, social services and policing break European law, and are in many cases unlikely to bring the stated benefits in any case.

It is typical for such systems to be built for utilitarian goals but justified to the public with emotional appeals. For example, the children's databases were marketed with appeals to the memory of Victoria Climbié, even although in that sad case all the information was available; the professionals involved had simply failed to act on it. Eventually Kevin Brennan, Parliamentary Under Secretary of State in the Department of Children, Schools and Families clarified in response to a query from a member of the public about ContactPoint:

'In your letter, you assert the Government is introducing ContactPoint chiefly to prevent another terrible case like that of Victoria Climbié. This is not the case. The chief purpose of ContactPoint is to improve the efficiency of children's services by freeing up practitioner time.'

The point is of course that while the Government may legally disregard consent in order

---

[1] *'Children's Databases – Safety and Privacy'*, R Anderson, I Brown, R Clayton, T Dowty, D Korff, E Munro, Information Commissioner's Office, Nov 2006; at http://www.fipr.org/childrens_databases.pdf

to save life, it may not do so for simple administrative convenience. Mr Brennan's admission rather undermines the legal justification for ContactPoint.

The latest development is the announcement on February 13th that, with the full backing of the Information Commissioner, the Government will construct a national database of schoolchildren's personal details, including not just test results but disciplinary matters – and that this database will not only be kept forever but will be made available later to universities and employers[2]. If this announcement is accurate then the Information Commissioner's support is deeply disappointing. Our report to him explained in detail why, as the regulator, he should not support such a scheme. We do not propose to repeat the reasoning here; we will just remark that in Germany, for example, it is unlawful for a primary school teacher to tell a secondary school teacher the marks obtained by a pupil going up to the senior school. It is accepted that children should have a fresh start in a new institution; both performance and behaviour have a significant situational component, and low marks from one school are known to depress expectations in a new school, leading to suboptimal outcomes. Given this, there is little prospect that a utilitarian argument can overcome the strong presumption of privacy in the underlying law. We reiterate that European human rights law, which leads German regulators to these conclusions, is also law here – regardless of whether the Government chooses to pay attention to it, or whether the Information Commissioner regards himself as required to give effect to it. Eventually, we suspect, a European law challenge will be needed in order to uphold the privacy rights of UK citizens. This is not an optimal way of conducting policy. It will be hugely expensive to remove or redesign significant numbers of public-sector systems once it can no longer be disputed that they are unlawful.

Healthcare Systems

Many public-sector applications might be affected by this review, but probably the most important is healthcare. The systems being developed under NPfIT will collect massive amounts of personal health information centrally, without patient consent and without the practical possibility of opting out. Some have welcomed this as a major opportunity for UK medical research. Yet the proposed trade-off between privacy and medical progress is simply not available for the Government to make – unless it is prepared to withdraw Britain from the European Union, and perhaps the ECHR. The compulsory collection of our medical information in the absence of consent, and even in the face of persistently expressed refusal, is illegal as well as unethical. This position is supported by numerous international conventions and resolutions (such as the Declaration of Helsinki, the Council of Europe recommendation R97(5) and the Article 29 Working Party WP 131).

We deal with the legal issues in detail in our report on children's databases, insofar as it applies to under-18s; the situation with adults is not hugely different. With children's databases we documented many abuses of the consent process, from disregard of the law

[2] "Every child in school numbered for life", A Frean, Times, Feb 13 2008; at http://www.timesonline.co.uk/tol/news/uk/education/article3359931.ece

that the parents of children under 16 should be involved in consent unless the children request otherwise, through presumptions of consent, to outright coerced consent. The same sad pattern is established in healthcare; not only are patients presumed to have consented to information sharing by virtue of seeking treatment, but patients who refuse consent may be threatened with degraded treatment or even denied treatment.

As far as public opinion is concerned, repeated research studies[34] have shown that most British citizens (like Americans and other Europeans) are content to have their information used in research, provided they are asked; they will resist if information is simply taken. Implied consent is seen as no consent.

Yet the Department of Health has made repeated attempts since 1910 to get hold of all British medical records. Two of us (Anderson and Fisher) have experience going back into the 1990s when the previous attempt (the IM&T strategy) was made by a previous health secretary (Dorrell). On that occasion, a 'single electronic medical record, shared by all in the NHS' was sought; the real reason appeared to be a combination of a power struggle between administrators and doctors, coupled with general administrative hunger for access to information. Of course, it was dressed up with appeals to the benefits of research, and the story of 'if you fall ill in Aberdeen …' (we will do Dr Walport the courtesy of not bothering to roast that old chestnut). Doctors were not convinced and the plan was abandoned.

NPfIT differs from the previous attempt only in that this time a Prime Minister committed billions of pounds to trying to actually implement the scheme. The resulting chaos has been well documented in the press[5] and by the Public Accounts Committee[6]. The Health Committee made various recommendations that ministers have resisted, notably that 'sealed envelope' information should not be made available to Secondary Uses Service (SUS)[7]. This would have given patients a route whereby they could opt out of having their data used for research; now it would appear that (for example) a religious lady who objects on principle to her gynaelogical data being used to develop better abortifacients has no choice but to seek treatment privately (or perhaps abroad) for any gynaecological complaint.

---

[3] "Clinical Systems Security – Implementing the BMA Policy and Guidelines", A Hassey, M Wells, in *'Personal Medical Information – Security, Engineering and Ethics'*, RJ Anderson (editor), Springer (1997)

[4] *'Public Perspectives on the Governance of Biomedical Research: A qualitative study in a deliberative context'*, V Artmstrong et al., Wellcome Trust (2006), at http://www.wellcome.ac.uk/assets/wtx038443.pdf

[5] http://www.nhs-it.info

[6] *'Department of Health: The National Programme for IT in the NHS'*, Public Accounts Committee (March 2007), at http://www.publications.parliament.uk/pa/cm200607/cmselect/cmpubacc/390/390.pdf

[7] *'The Electronic Patient Record'*, Health Committee (September 2007), at http://www.publications.parliament.uk/pa/cm200607/cmselect/cmhealth/422/42202.htm

The case of Helen Wilkinson has helped underline how difficult life now is for a patient who refuses on principle to share her medical information with the state. Where treatment is at an NHS hospital, or at a private hospital but paid for by the PCT, a summary of each finished consultant episode ends up on the SUS database, which is widely used for service planning and research. Although in law patients are able to opt out of this, the UK implementation requires them to use Section 10 of the Data Protection Act, which the Department makes as tiresome as possible. In Helen Wilkinson's case, it took an adjournment debate in Parliament to extract from a health minister the assurance that her data had been removed from the system[8]. (The assurance turned out to be false; the minister in question has not apologised and has continued her career in another department.) Systems appear to be designed in such a way that someone getting hospital treatment will have their data sent to SUS, like it or not[9]; the best they can do is to agitate after the fact for an assurance that it has been removed, with no effective means of enforcement or verification.

GP treatment remains in many cases moderately private but this is being severely eroded. Many GPs have been bribed to move to centrally hosted systems; their data are no longer in the surgery but sitting on a remote server farm controlled by a government contractor. The government's declared intention is to share this data across the local health community, to copy it to SUS, and to share it with other departments (see our report on children's databases). This is clearly illegal. Also, as a matter of fact rather than of law, the GP no longer has control. This will make access by third parties much easier in future. At present, a policeman wishing to check a suspect's record to see whether she had admitted drug use to her doctor must get authorisation from a Crown Court judge, then present this to the doctor. In future a Chief Constable will be able to seek a single order for the production of all records relating to drug use in his area (which a judge ignorant of European law might well grant as UK law presently allows access to 'actual evidence of crime'), present it to a manager at BT, and leave the doctor none the wiser[10]. This is not a fanciful scenario: we know of a police demand to a pregnancy advisory service for information on their under-16 clients. In that case they were told to get lost, and didn't press the point; but a manager at a data warehouse whose client is the Government of the day is likely to react differently from a practising gynaecologist who sees her patient relationships, professional integrity, self-esteem and business viability all directly under threat from such a request.

Even where GPs retain control of patient records, the Quality and Outcomes Framework (QOF) that rewards them for meeting Government targets already causes significant

---

[8] Adjournment debate of June 16 2005, at http://www.publications.parliament.uk/pa/cm200506/cmhansrd/vo050616/debtext/50616-37.htm#50616-37_spmin0

[9] FIPR submission to Health Committee on the Electronic Patient Record (EPR61), http://www.publications.parliament.uk/pa/cm200607/cmselect/cmhealth/422/422we22.htm

[10] "Patient confidentiality and central databases", RJ Anderson, British Journal of General Practice v 58 no 547 (Feb 1 2008) pp 75–76(2)

privacy compromise. One of the writers recently changed GP; the new GP's first question was 'Do you smoke?' Being aware that this is data that GPs are paid to collect for the Department, and not relevant to the presenting complaint, the immediate response was 'That's none of the Secretary of State's business.' That is hardly the way to start a new doctor-patient relationship. Yet as knowledge of NHS data 'sharing' becomes more widespread, such encounters will become more frequent.

In short, the centralization and 'sharing' (we'd prefer the phrase 'unlawful privacy compromise') of the nation's medical records are a bridge too far. Even the existing practices – let alone the planned ones – are in many cases not only unethical but unlawful. They undermine trust in the doctor-patient relationship and compromise patient care directly. People ignorant of NHS information practices, who become aware of them, mostly find them repulsive. The program is foundering, and could be destroyed outright if a single litigant had the money and the guts to go to Europe. The Conservatives have promised to abolish the system, along with the ID database, if they win the next election.

If, in the meantime, medical researchers have come to depend on these systems, the disruption will be severe. In addition to losing access to data, researchers risk losing public acceptance of their work and may even find the publication of their work objected to overseas on ethical grounds.

Under the circumstances we find it profoundly unfortunate that Dr Walport should continue to advocate that UK citizens be compelled to hand over our medical records for the benefit of 'research'. Such political advocacy is in any case in conflict with the Wellcome Trust's charitable status. Organizations that pursue both charitable purposes and political lobbying – such as Liberty, and Privacy International – have to take great care to divide their operations into a charitable part and a lobbying part, and not subsidise the latter with funds raised for the former.

We also invite Dr Walport to contemplate two precedents. First, the inhumane treatment of laboratory animals until a generation ago spawned the Animal Liberation Front. Second, the cavalier treatment of human body parts led to the Alder Hey scandal. In each case, medical researchers acted as if they felt that the exceptional value of their work put them above other considerations. In each case, they and their successors have paid the price of this exceptionalism. Thus even if the Wellcome Trust believes that medical research is the highest good, advocating compulsory data collection is not a prudent way to promote it.

Many would of course argue that privacy is a greater public good than medical research. The therapeutic benefits of confidentiality are real, and many patients already die because they do not seek treatment early enough for dread diseases from HIV to cancer. The extra benefits to research of compulsory collection, over and above what can be achieved by asking for consent, are unclear. Even if we do not advocate such an absolute view here, we consider that no scientific case has been made for a need to privilege research above the clear need for medical privacy.

Action

Assuming that the UK will remain part of the European Union and continue to adhere to the ECHR, the real question is whether the privacy rights we enjoy by virtue of being European citizens are to be enforced by private action or public action. Up till now the presumption has been in favour of the latter. But although this approach has worked tolerably well in many other Member States, it has not worked here. Successive holders of the office of Data Protection Registrar or Information Commissioner have bent to the will of the Government of the day, and taken a stand only when they would have been discredited otherwise.

To be fair, the then Home Secretary David Waddington remarked of the passage of the first Data Protection Act (1984) that it was a minimum implementation to keep us compliant with the UK's international obligations; and a former Cabinet Secretary told one of us that such regulators were a tiresome necessity of the modern age, best dealt with by starving them of funds. We should state that we also mean no personal criticism of the current Information Commissioner; many members of the FIPR Advisory Council could credibly have applied for his job when it was last vacant, and none of us did.

The first option is to fix the Information Commissioner's Office. FIPR has at various times in the past supported this option, which might involve giving the Information Commissioner the independence of a High Court judge (tenure until a fixed retirement age, removable only for misconduct and by a vote of both Houses of Parliament, funding authorised directly by each Parliament for its successor). However there would remain an issue of culture change. The ICO now has a large established policy staff who appear to see their duty as primarily to their 'stakeholders' in Whitehall, and their mission as facilitating public-sector information sharing by reassuring the public, rather than upholding privacy rights. There are two ways in which regulatory capture of this severity might be tackled. The first is external action: a Prime Minister determined to fix privacy but retain public action might abolish the existing ICO, make its staff redundant, and start afresh with new people in a new office in London. The second is internal action: the Information Commissioner might start to enforce data protection law extensively and intensively insofar as he is empowered by Parliament to do so. Where he is not able to do so, because of the defects in the Data Protection Act, he should not just condone unlawful conduct, but declare it to be unlawful and invite interested parties to litigate. Such a change in strategy would send a strong signal that internally-led change could productively be supported by Parliament.

The second option, to which we are now starting to lean, is that privacy rights should be enforced by private action rather than public action. At present, it is extraordinarily risky for private individuals in Britain to take a test case against a government department, because of the rule that the loser pays the winner's costs. In America, where each side pays its own costs, there is no shortage of law firms and NGOs ready to take test cases under the Constitution; even in Germany, where court rules limit the losers' liability much more tightly than here, private action is feasible. In England, however, such cases are generally limited to legally-aided matters. Thus human-rights law has been largely

limited in its development to matters relevant to criminal defendants, applicants for housing or welfare, and wealthy corporate litigants. FIPR believes this is wrong. Limiting access to justice in a discriminatory manner is bad enough; limiting access to the enforcement of fundamental constitutional rights is intolerable.

FIPR believes the UK should adopt the US rule that each party to a civil case should pay its own costs. If that is felt too ambitious, then a minimal implementation would be to shield from costs orders all litigants who bring a case founded on the ECHR unless perhaps they are found to have litigated vexatiously.

Finally, we urge the Wellcome Trust to adopt a policy that it will fund only research that is both ethical and lawful. Regardless of any potential clinical benefit, it should refuse to fund any UK research that will use data collected without proper informed consent.

Ross Anderson
Nicholas Bohm
Terri Dowty
Fleur Fisher
Douwe Korff
Eileen Munro
Martyn Thomas

February 15 2008