Inquiry into ‘A Surveillance Society’

Foundation for Information Policy Research (FIPR)

Response to the Home Affairs Committee

The Foundation for Information Policy Research 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 were asked by the adviser to the Home Affairs Committee to submit evidence on the large strategic issues of concern to the general public raised by the numerous public and private databases and forms of surveillance with a direct relevance to the work of the Home Office, including ‘the databases being developed by the Department of Health and the DfES for use in the fight against crime’.

We would like to make the following points.

1. The UK does a lot more surveillance than other countries, especially when it comes to CCTV. This raises, at the very least, the question of whether the public money invested in these systems yielded a satisfactory return. In the case of CCTV the answer appears to be no: although CCTV is effective at reducing crime in car parks, where there are restricted exists, the evidence does not support its effectiveness elsewhere[1].
2. The origins of the overinvestment appear to be as follows. The Criminal Justice and Public Order Act 1994 allowed local authorities to establish CCTV systems in order, inter alia, ‘to promote the prevention of crime’. The current government started off well enough in 1997 with its ‘Comunities that Care’ initiative, under which local community leaders meet and suggest neighbourhood initiatives that would in their opinion reduce crime – which might include anything from better street lighting to improved sports and play areas. However, this appears to have become entangled with the CCTV initiative with the result that instead of subsidising ‘initiatives that would make your neighbourhood safer’, the Home Office has been subsidising ‘initiatives that would make your neighbourhood safer using CCTV’. As a side-effect, the ‘Communities that Care’ initiative appears to have languished, or at least been much less effective than the US pilots on which it was based. The Committee should therefore consider not just the waste of public funds but also the opportunity costs – the better crime-reduction initiatives that were crowded out.

[1] M Gill, A Spriggs, “Assessing the Impact of CCTV”, Home Office Research Study 292, february 2005; see also their other publications at www.perpetuitygroup.com

3. Once these lessons are learned, we may expect that in future there will be less CCTV surveillance. However there will still be some, and the Committee should next consider the issue of access to and processing of stored image data. In the past there have been some notorious abuses (including operators selling images of people having sex). The Data Protection Act 1998 empowers the Secretary of State to order 'assessment' of processing operations that 'appear[] to him to be particularly likely – (a) to cause substantial damage or substantial distress to data subjects, or (b) otherwise significantly to prejudice the rights and freedoms of data subjects' (Section 22(1) DPA98). Justice has called for data matching CCTV cameras and facial recognition software in particular to be designated as 'assessable processing. Unfortunately no such order has been issued.
4. We would like to raise an important point that we believe has been overlooked. Strategic issues raised by CCTV (and other forms of surveillance) are not limited to privacy, but extend to equality of arms in both criminal and civil cases. It is much easier for the police to get access to CCTV images to prove guilt than it is for a citizen to get access to establish an alibi; and in civil disputes involving (for example) disputed ATM withdrawals, a customer in dispute with her bank will typically find it impossible to get the relevant CCTV images.
5. We suggest that committee members read David Brin's book 'The Transparent Society', which argues that given the dramatically falling costs of data acquisition, storage and processing, we face a choice of two futures: one in which the government knows everything about its citizens who are disempowered and alienated as a result, and an alternative in which citizens can also observe the rulers (and each other). Brin argues for the abolition of most forms of privacy; he suggests not only that anyone should be able to read anyone else's bank statements, but even that anyone should be able to tap anyone else's phone. While Brin takes an extreme position to make his readers think, his position contains a kernel of truth. A world in which the spooks know everything, the police know almost everything, the banks and credit reference agencies know an awful lot, and the citizens know very little, will not be the same as the Enlightenment vision of a democracy of citizens equal under the law.
6. Parliament's historic attempt at balance was the Freedom of Information Act, which made the Information Commissioner responsible for encouraging the flow of information to the ruled about the rulers as well as for limiting the flow to the rulers about the ruled. This is inadequate for two reasons. First, there are constant pressures on governments in the other direction, so the balance is steadily eroded. Second, such a dispensation is essentially a centralising one. State action displaces private action: only the state has the information needed to act.
7. For example, the Government has struggled for years to make the Child Support Agency into an efficient vehicle for recovering a certain kind of civil debt, namely alimony. In the process it has caused much misery. We suspect the solution must be to give citizens better mechanisms to recover civil debts of all kinds. Thus a divorcee seeking to enforce a court judgement should be able, by court order, to track down a fugitive partner, identify his registered assets from bank accounts through motor vehicles to real property, and seize what is due to her. Similarly, as technology makes it simple to keep CCTV images forever rather than just for a

week, someone wishing to establish that they did not make a disputed ATM transaction, or to establish an alibi in a criminal matter, should be able by order to access the relevant images.

8. Transparency and equality of arms would go a long way in ensuring that public support for surveillance is retained in the long term. The same applies to access to databases; information sharing between public sector bodies and private agencies will be undermined if the exercise is seen as favouring big companies against small firms or individuals, or the strong against the weak generally.
9. Matters will be even worse if large quantities of public-sector data start flowing to the private sector; government datasets are notoriously inaccurate, and if they start being used by credit reference agencies and banks in lending decisions, then innocent people will be harmed. If, at the same time, more and more government departments start using credit reference agency data, there is a clear risk of positive feedback loops whereby some wrong information on a citizen, whether entered accidentally or maliciously, contaminates a number of public and private databases, making some poor citizen's life a misery. In a world of pervasive and growing 'identity theft' this is not acceptable.
10. We put the term 'identity theft' in parentheses because we don't agree with it. Ten years ago, if someone went to the Midland Bank, pretended to be me, borrowed £10,000 and vanished, that was the crime of impersonation; it was the bank's problem rather than mine. Now it's called 'identity theft' – supposedly it's not the bank's money that's been stolen but my identity. This suits the banks as it help them dump fraud liability on customers, and it suits the Home Office as they think it will help them sell identity cards.
11. But from the point of view of data protection, the problem is that credit reference agencies knowingly pass on false information about the 'victims' of 'identity fraud' even although they know that the victims have nothing to do with it. When challenged, the agencies say that they are simply holding this data on behalf of the banks. This is untrue as in law they are the data controllers, and by passing on false information they break the fourth data protection principle. They are also committing a civil libel. The Information Commissioner should be ready, on application from a victim of 'identity theft', to issue an enforcement notice against the agencies committing the defamation. Unfortunately, successive Information Commissioners have proved reluctant to act. That must change if more public-sector use is to be made of agency data (and indeed in any case).
12. On the topic of 'identity', a controversial bundle of issues centre on the ID card system and the identity register that will stand behind it. FIPR gave evidence to the Committee on this topic in 2004; we refer the Committee to that evidence and also to the LSE report warning about the project's likely costs[2] – which seems more prescient with every new cost escalation. We remain deeply sceptical about this project. Recent research[3] also strongly suggests that the obsession with

[2] "The Identity Project – as assessment of the UK Identity Cards Bill and its implications", LSE, June 2005; at csrc.lse.ac.uk/IDcards/identityreport.pdf

[3] 'Closing the Phishing Hole: Fraud, Risk and Nonbanks', Ross Anderson, Federal reserve Santa Fe Conference, May 4–6 2007; at www.ross-anderson.com

identity since 9/11 has damaged the fight against fraud and money laundering; 'follow the man' and 'follow the money' are not perfect substitutes, and an overinvestment in the first has caused the neglect of the second.

13. The Committee asks about the potential abuse of private databases by criminals. Honourable Members should also consider the abuse of public sector databases; there has been considerable concern, from the public to senior police officers, about potential abuse of the proposed identity register. It is already the case that public sector databases are unlawfully accessed on a regular basis by private detectives and others, especially when they wish to trace people.
14. Two members of FIPR's Advisory Council were involved with the BMA in an experiment in 1996 to determine the extent of abusive access to NHS data. Staff at the North Yorkshire Health Authority were trained to detect and deal with false-pretext phone calls, by logging calls requesting personal data and calling back to a number found in a phone book rather than to the number given by the caller; this simple authentication mechanism revealed some 30 false-pretext calls a week. The BMA asked the Department of Health to extend these operational security measures throughout the NHS; its response was to order the NYHA to cease and desist. No doubt many people have been traced, and/or had their personal health information compromised, since then.
15. The new Population Demographics Service in the NHS will make it easy for any NHS staff member to trace anyone in the country, including ex-directory numbers (although it is possible to opt out of PDS, you then cannot use Choose and Book or electronic prescriptions). The identity register, if built, will no doubt be used for similar purposes. The Police National Computer has long been abused by corrupt or careless officers despite a substantial audit resource and frequent prosecutions; public-sector databases accessed by staff under less discipline, who are audited less rigorously, and who work for organisations that care less about security, will likely be abused more.
16. Thus, at present, the state's ability to trace people is made available to private individuals through unregulated and largely unlawful means. This facilitates various sorts of harm, from the harrassment of celebrities to intimidation of witnesses and vengeance against former partners' lovers. We propose instead that there should be properly regulated mechanisms for tracing individuals and assets. This should remove much of the demand from private investigators for access to such material. Draining the swamp will surely be better than giving a short jail sentence to the occasional crocodile.
17. The Committee asks about Home Office use of health and education databases. FIPR wrote a report "Children's Databases – Safety and Privacy" for the Information Commissioner in 2006[4]. There we documented the government's plans to link up databases with information on children, including NHS, social work, police and education systems. A key driver is the Home Office belief that future delinquents and offenders can be identified and targeted for early intervention. We are deeply sceptical about this; it is extremely likely that the costs will greatly outweigh any benefits.

[4] Available from www.ico.gov.uk and from www.fipr.org

18. The Committee asks about ‘Profiling’; we’d suggest it consider the analysis set out in our report. It is very hard to predict which children will offend, and the attempt carries a serious risk of stigmatisation, so that predictions can become self-fulfilling. Many young people successfully overcome multiple disadvantages, such as a bad neighbourhood, a single-parent family and poor health; marking all multiply-disadvantaged youths as ‘likely to offend’ is unjust. Equality activists have long talked of the ‘offence’ of ‘driving while black’; the risk of profiling is that young people in future may be pulled over for ‘driving while having more than 60 points on the ONSET system’. If vulnerable young people are repeatedly stopped by the police, or treated like suspects rather than witnesses whenever they come to attention, then they can easily be driven to rebellion and criminality.
19. Quite apart from the law-enforcement aspects of child surveillance, there are grave doubts about its effectiveness in social care. There is a shortage of effective interventions, with Communities that Care and Sure Start having been largely ineffective; there is a serious risk of losing the confidence of social workers, teachers, doctors and other professionals, and of compromising public confidence in the confidentiality of health and social services. (This trust has proven therapeutic value.)
20. In short, the costs of widespread information sharing on children appear to greatly exceed the benefits. Even if officials argue that they can predict from surveillance who’ll offend, there are much easier ways to identify troublesome kids (just ask the teachers); but it’s not easy to do anything about them, and it’s not Home Office turf anyway. It’s pointless to do surveillance and not be able to act on it, and action is the hard part. Furthermore, a number of the proposed information flows are contrary to European (and thus UK) law.
21. Another example of police use of health data goes back to 1996, when there was a tussle between the government and the BMA over granting the police access to the Prescription Pricing Authority database. This was sought with the argument that the police needed to track down the small number of doctors and nurses who abuse their ability to prescribe opiates. Eventually the BMA decided not to fight the issue, and conceded police access. Yet Dr Shipman kept on murdering his patients for several years after that. The Committee might care to ask ministers how this happened. This may help bring home that simply sharing data between government departments and agencies does not by itself mean that anything useful will be done with it. As well as the data, there must be mechanisms, systems and above all incentives; for the police, the PPA data may have been ‘nice to have’ but trawling it was presumably not a priority as they didn’t know that a Shipman existed. Perhaps if the GMC had been assigned the surveillance task, Shipman would have been caught sooner.
22. The committee asks about ‘Existing safeguards for data use and whether they are strong enough’. The brutal answer is that UK data protection law has always been not only weak but defective. This is not a party political issue; data protection acts introduced by both parties have equally failed to give effective force to European treaties and law. This is explored in detail in chapter 7 of our report on children’s

databases[5]. The effect in healthcare is that while everywhere else in Europe governments consider it necessary to get patient consent for secondary uses of health records, here in the UK it is considered sufficient to offer some limited (ineffective) patient opt-out from some of the applications. The risk is that a future European law challenge will undermine NHS business processes that by then might be expensive to change. (This matter is currently being considered by the Health Committee, which is due to report in July.)

23. The Committee asks about monitoring of abuses. As we remarked above, the PNC is the one public-sector database where a real effort is made to catch abusers, and even that doesn't stop abuse. In the NHS, privacy breaches are not reported to patients but to 'Caldicott Guardians', typically senior managers who have every incentive to cover up problems in the absence of clear evidence of actual harm. The only way to get the incentives right is to notify patients, as is done in many other countries. Indeed FIPR believes that the UK should have a security breach disclosure law, as exists in most US states; any organisation suffering a breach of systems security should be compelled to notify all data subjects whose information may have been affected. This is desirable for many reasons other than privacy; for example, people whose credit cards have been compromised should be told so that they can have them reissued[6]. (There is an EU proposal for a directive on security breach notification, but it's limited to telecomms; this is one area in which the UK legislator could usefully go farther and faster than Brussels.)
24. FIPR also testified to this Committee in 2006 about forensic problems caused by the growing volumes of data seized nowadays and police inability to cope. We mentioned that Operation Ore had caused particular problems by its extravagant resource consumption. Recent revelations about the incompetence (to put it at its most charitable) of that operation are deeply disturbing: it appears that about two thousand people were raided by the police during 2002–6 on suspicion of having downloaded child pornography when in fact they had simply been victims of credit card fraud. Security breach disclosure laws will help prevent a repetition of this (though many other things are needed too, from better police forensics through to punishment of the culprits in that particular case).
25. Action is needed to make the Information Commissioner's Office more effective and to make proper penalties available for abuse. First, the ICO has always been lacking in technical capability, which has undermined its credibility. Second, the proposed changes to data protection law, agreed by the ICO and the Ministry of Justice, provide for (short) prison terms to be available for private detectives and others who gain improper access to data, but not for the data controllers who give them this access. This is also unsatisfactory. In fact, we think that the ICO needs a radical rethink; Parliament should consider the proper allocation of the regulatory tasks currently performed by the ICO, the various surveillance and intelligence commissioners, and the IPCC. What governance structures are needed to ensure

[5] See also Professor Korff's testimony for FIPR to the Health Committee enquiry into the Electronic Patient Record

[6] See Professor Anderson's testimony for FIPR on this topic to the Lords' Science and Technology Committee enquiry into Personal Internet Security

that official access to information is not abused in the information age? What laws or institutions are needed to overcome or sidestep the civil service opposition to privacy and freedom-of-information laws that has undermined the ICO to date?

26. In summary, we're deeply sceptical about the notion that pervasive surveillance will solve social problems. It's been tried for over a dozen years, and we have yet to see the evidence that Britain has gained, say by comparison with Germany where privacy laws are better enforced. The huge investment in CCTV looks like a mistake, and spending billions more on identity registers, children's databases, ANPR, and other mass surveillance systems, is foolish. The vendors of these systems have mostly failed to make a case on costs and benefits.
27. There is also a deep political question about the relationship between the citizen and the state. A frequent objection to the ID card project has been that many people prefer the 'British way', whereby the policeman shows his warrant card to the citizen, rather than the 'German way' in which the policeman imperiously demands the citizen's *Ausweis*. Other mechanisms of surveillance and control will carry similar side-effects. We won't be able to predict them all in advance, but legislators should still have some guiding principles.
28. We'd therefore suggest that the Committee try to develop a vision of how citizens relate to the state, and to each other, in an information society. How should society regulate access to the masses of public and private sector data that are gathered, or that can be used for, surveillance? If there is going to be a 'British way', what should it be?

Professor Ross Anderson
Dr Ian Brown
Professor Douwe Korff
William Heath

Cambridge, May 21st, 2007