The Foundation for Information Policy Research and the Open Rights Group

Consultation response on

Interception Modernisation or 'Protecting the Public'

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.

The Open Rights Group (ORG) is a grassroots technology organisation that exists to protect civil liberties wherever they are threatened by the poor implementation and regulation of digital technology.

We would like to make the following response to the Home Office consultation on the Interception Modernisation Programme, entitled 'Protecting the Public in a Changing Communications Environment'.

First, we reject the claim that the ability of the police and intelligence services to collect intelligence and evidence is under threat. The last twenty years have brought investigators an absolute cornucopia of new sources and methods, as many acts that used to leave no record have moved online, and the records they leave become persistent and searchable. The most obvious example is that most people now carry mobile phones, leaving a record of their location history with their phone company; and an intelligence agency wanting to know "Who did Burgess socialise with at Cambridge fifteen years ago?" will in future just look on Facebook, rather than having to covertly track down and interview hundreds of contemporaries. Indeed, although a number of us attended IMP briefings both at the Home Office and at Parliament, we still fail to understand the problem for which IMP is supposed to be a solution. Perhaps GCHQ simply wants convenient access to all UK communications without having to produce any evidence of why such powers are relevant and needful, let alone proportionate and lawful.

Second, the consultation assumes that the solution to the problem (whatever it is) must be a large IT project. A recent history of the NSA [1] described the agency's experience of dealing with digital data, compared with the international phone and cable traffic of the old days. A few streams of simple data have been replaced by many streams of complex data; people send messages via all sorts of media (phone, text, email, Facebook) and from all sorts of places (home, work, cybercafes, …). A smart agency that exploits what's available can get vastly more take for a small budget than was possible before; but a rich and risk-averse agency that wants to collect absolutely everything faces an intractable system engineering task. This is particularly the case if you want to collect Facebook or

Second Life data not from the operators of those systems, but via ISPs: an agency that tries this will need to spend a lot of money and effort in understanding ever-changing ISP systems as well as the target systems of interest. In fact, the NSA had a massive project, Trailblazer, to collect everything. It started in 1999 and was abandoned in 2005 following delays and cost overruns. General Hayden admitted to the US Senate Select Committee on Intelligence, "We learned that we don't profit by trying to do moon shots … that we can do a lot better with incremental improvement." In view of the UK government's terrible record in dealing with large IT systems [2], GCHQ and the Home Office should simply abandon any idea of a 'moon shot' to 'fix' surveillance. Indeed, their attempt to sell such a project to ministers calls their judgment of realities seriously into question (regardless of what it may say of their opinion of ministers).

Third, as any real progress will be made incrementally, we have to understand what the current problems actually are. The main problem is keeping up with all the data that digitisation makes available. The arrest of even a small-time drug dealer can provide a couple of laptops, several mobile phones, iPods, memory sticks – terabytes of data that must be secured, searched, indexed and copied to defence solicitors. Captured devices are a major source of intelligence and evidence – even in terrorism cases. Yet there is a large and growing forensic backlog. As for 'network' as opposed to captured data, most of the usable evidence comes from phone logs – who called whom, when and where. Very little comes from Internet data; it can be of occasional use in intelligence (e.g. logs from child porn websites suggesting whom to investigate) but is often not reliable enough to be used on its own as evidence (the apparent porn user might just be a victim of credit card fraud). From the police point of view, what's actually needed is a lot more money for politically unglamorous operational stuff – better computer forensics, better training, and more international cooperation [3]. Although the proposed database would make complex enquiries faster and cheaper, there aren't enough of them to justify it.

Fourth, the proposed wide deployment of deep packet inspection (DPI) technology raises many serious questions. DPI is already used by intelligence agencies to reconstruct traffic such as webmail from the data they intercept off high-speed links. Reference [1] describes some of the shadowy firms and deals in this space. The wide deployment of DPI by a democracy for internal policing, as opposed to its use on international links for foreign intelligence, would provide less intelligence and evidence than one might think, while causing serious legal and political problems.

- DPI equipment struggles with encrypted traffic. The use of encryption is increasing rapidly because of the music industry's war on peer-to-peer file sharing. Options are (a) let people encrypt their traffic if they want (b) do a man-in-the-middle attack, as Burma does (c) ban crypto, as Tunisia does. Democracies have chosen (a), and the use of crypto is embedded in too much architecture for this to change. Knowledgeable villains will continue to use skype, encrypted gmail, throwaway mobiles and whatever comes next.
- Coverage will be less than 100% for volume reasons. In practice, GCHQ would have to tell the ISPs which traffic was of interest, so they could store it. Now GCHQ doesn't trust the police: knowledge of what's been collected will leak data

about intelligence tasking and will thus be SECRET. This means that ISPs may not be able to give the police data they have on their premises even though it would be helpful in murder or child-abuse enquiries! What's more, the Home Office don't seem to be able to take a view on whether ISPs will be able to use the collected data for their own purposes. Officials seem inclined to say no – though how the ISP is supposed to collate the take with its own data, e.g. to identify customers, seems rather unclear. (In fact, the design is a complete mess.)

- The DPI boxes will be reprogrammable by GCHQ, which will raise serious control issues and exacerbate public distrust of the intelligence community. It will be natural for GCHQ to harvest content as well as traffic data, so reasonable people will not believe assurances that "this is only about communications data". And even if some way could be found to verifiably prevent GCHQ (or anyone else) from harvesting content through the DPI network, traffic data can be hugely intrusive. (Just think about online porn video rentals, or a newspaper leaking MPs' web browsing habits.) Its pervasive collection and analysis, from innocent citizens as well as suspects, will almost certainly be illegal under ECHR [2]; in Germany, even the current data retention regime is under fire in the courts.
- If GCHQ intends to do snowball searches and run other distributed data mining algorithms, this will need large numbers of high-speed accesses to ISP databases, which the ISP will not in practice be able to control. Essentially the system will be a distributed implementation of the previously-proposed central database, located on ISP premises, but completely controlled by the centre.
- The costs will be huge. Modern ISPs have large complex networks; there is no longer a single LAN to which a Carnivore box can be attached. The Home Office claimed in briefings that the project would cost £2bn, but would give no justification. This is just implausible. We expect it would cost at least £10bn.
- DPI equipment can also be used to monitor political speech, and is indeed used by repressive regimes for this purpose. The next Government should think hard about whether we want the UK to build the kind of network infrastructure that's being built in countries like Iran [4].
- Pervasive DPI will put UK plc at a serious competitive disadvantage. The only other country to have attempted this is Sweden; Finland and the other Baltic states have reacted by rerouting their email and other traffic to avoid it.

This leads us to our fifth point: the consultation suggests that GCHQ sees its future in domestic rather than external intelligence. This shift is at least as important as any of the technical matters raised. In the past, GCHQ has had considerable freedom of action, like the NSA. If its future targets are not the Russians, the Chinese and the Persians but us, then its future model should be the FBI instead. It must be a more open and disciplined service, operating under judicial warrants and close parliamentary scrutiny. However a review of its accountability mechanisms is unlikely to be enough. If ministers come to believe that the main future security threats to the UK are internal, much else follows.

At the very least, the next Government should conduct an ab initio strategic review of the intelligence services. Do we need three services, or two, or four, or five? If foreign and domestic services are to remain distinct, should each have its own technical capability in-

house, in line with the broader philosophy of mainstreaming computer capability within police forces and elsewhere, or should there be a separate technical service for each? We suspect that domestic technical intelligence may come to depend on lawful access to retained data while external intelligence may involve covert collection and international trading more than anything else. These methods involve quite different skill sets, infrastructure and accountability issues. In addition, the protective service, CESG, has an awful record; it's time it was separated from GCHQ so that future Governments can protect public-sector data properly against attacks.

Finally, we do not agree with the Home Office rhetoric that they must "protect the public" and that "doing nothing is not an option": we reject the premise that "terrorism" is a serious or existential threat to the UK that justifies the infringement of human and other rights. The Soviet strategic rocket forces may have been an existential threat, and the IRA may have been a serious threat; by comparison the threat of occasional bombings by deluded young Muslims is low-grade. (The fatality risk is less than one in a million per annum; thus, under health and safety guidelines, the threat could simply be ignored.) Political violence has always existed, and civilised states must find ways to deal with it. In our view the best approach is that followed by Mrs Thatcher – downplay the risks and treat offenders as criminals. Intelligent observers agree that recent infringements of rights have simply made things worse. The British Government should stop trying to "scare up the vote", as President Obama put it, and follow his lead in accepting that the "War on Terror" is over. It might even follow his lead in curtailing the wiretapping of citizens.

We hope that the next Government will turn over a new leaf. Since the UK joined battle in the crypto wars in 1998, many of the smartest people on the net have been figuring out ways to frustrate the spooks. It's time to get the geeks back onside, so they can spend their energies helping to catch the few really bad criminals instead.

Ross Anderson FRS FREng
Foundation for Information Policy Research
Cambridge, July 2009

Jim Killock
Open Rights Group
london, July 2009

References

[1] James Bamford, *The Shadow Factory*. Doubleday, New York, 2008.
[2] Ross Anderson, Ian Brown, Terri Dowty, Philip Inglesant, William Heath, Angela Sasse, *Database State*. Joseph Rowntree Reform Trust, 2009.
[3] Ross Anderson, Rainer Böhme, Richard Clayton and Tyler Moore, *Security Economics and the Internal Market*. ENISA, March 2008.
[4] Christopher Rhoads, "Iran's Web Spying Aided By Western Technology'', *Wall Street Journal*, 22/6/2009, at http://online.wsj.com/article/SB124562668777335653.html