Inquiry into Terrorism Detention Powers

Foundation for Information Policy Research (FIPR)

Response to the Home Affairs Committee

We were asked by the adviser to the committee to submit evidence on:

- the need to decrypt computer files;
- the length of time needed to obtain and analyse data from mobile phones;
- problems in dealing with growing masses of digital forensic material.

We have been shown submissions by Assistant Commissioner Andy Hayman and by Peter Sommer. We should point out that Peter Sommer is also a member of FIPR's Advisory Council and has been consulted on this response.

We would like to make the following points.

1. Modern cryptography tends to break quickly or not at all – either the data were encrypted using a bad product or a good one, and in the latter case you either guess the password or give up. Depending on the tools in use, it might take a few hours to a few days to try a large database of possible passwords on seized material; one tries out various dictionaries, girls' names, names of Premiership footballers, etc. (There are one or two products that still use medium-strength cryptography, but they are becoming obsolete: and even in these cases, cryptanalysis is easy to parallelise, in that a key which takes a month to break on a PC can be broken in a day on 30 PCs if the matter is urgent.) Thus cryptography per se does not justify an extended pre-charge detention period.
2. Obtaining data such as call logs and location history from phone companies under the RIP Act should be a fairly rapid process, as the information is stored on automated systems and there are established procedures for law enforcement agencies to work through single points of contact with the companies. While there may occasionally be delays, there are now procedures for expedited access when a matter is urgent. There is thus no good reason why access to traffic and location data should justify an extended pre-charge detention period.
3. We are concerned, though, that by concentrating on low-level operational aspects such as performing cryptanalysis and getting data for traffic analysis, the police may be missing the larger strategic picture, as follows.
4. The amount of data available in trials, both civil and criminal, is increasing much more rapidly than the capabilities of police, prosecutors, defence lawyers, and even lawyers in civil cases. Investigators are trying to drink from a fire hose, and the volume is being turned up all the time.
5. For example, Operation Ore presented the UK police with a list of 7000+ people who had bought pornography from a site in Texas that contained, inter alia, illegal images of child abuse. It also contained material that was merely tasteless. Much of Britain's computer forensic capability has been tied up for the last three years

in searching through confiscated PCs, trying to determine which type of images their owners purchased. Often evidence could not be found, and in some of these cases suspects may have been bullied into accepting cautions for 'incitement to distribute' to get the cases off the books. The recent headlines about teaching blacklists are just part of the fallout from that practice.

6. As another example, I am currently an expert witness in a civil matter in which the receiver of a failed company obtained a search order against a former director and seized ten PCs. Five months later, subsidiary litigation is underway about searching this material and the protocols for access. Civil litigation also results in huge volumes of data being obtained as part of the discovery process. A minor contract dispute can throw up 10,000 emails, while the US class action against tobacco companies generated over 10 million pages of documents. If the only way you can deal with that is to pay lawyers £200 an hour to read them, then litigation will become even more the preserve of the rich. One might draw a comparison with warfare, where the costs (and capabilities) of platforms such as combat aircraft have increased by orders of magnitude since World War 2.
7. This is not to decry the importance of digital evidence and intelligence. Indeed, it is the very usefulness of such material that has led police forces round the world to seize material in ever-increasing quantities, with the result that the existing analytic capacity is badly overstretched. Technological progress – the data storage equivalent of Moore's law – ensures that there will be ever-larger quantities of material to be seized. 'Pervasive computing' – the process whereby processors and communications are embedded in ever more everyday devices, from TVs to cars – will ensure that ever more devices contain digital records that might potentially incriminate or exculpate a suspect. It is likely that within 5-10 years a search of a single home or small business will yield the thousands of gigabytes of data apparently encountered by the police in the wake of the July bombings.
8. New things can be done with digital evidence. For example, one can 'undelete' files and email on seized computers, and perform rapid automatic searches for 'known suspect' email addresses, phone numbers and even pornographic images.
9. However, neither the tools available to analyse this data, nor the UK police forces' capabilities in particular, have kept up with technology use by suspects.
10. Today's tools are designed to analyse a single hard drive at a time, using labour-intensive processes that do not scale well. They also do not usually support the kinds of analysis needed when a case involves large numbers of disk drives, such as correlation analyses to see which PCs were exchanging data with each other; recent academic research (Garfinkel) has shown the feasibility of such analyses. The task now is to design, build and deploy the tools.
11. FIPR has been concerned for years that UK police forces tend to devote less money, effort and priority to IT matters (such as computer crime and digital forensics) than would be socially optimal. This has also been the consistent (privately expressed) view of the most able practitioners within the system. A number of FIPR members have been involved in remediation activities ranging from police training to speaking at law-enforcement conferences.
12. In short, this is not a 'terrorism' problem, but a general problem.

13. The solution is unlikely to be found in extended pre-charge detention, even for terrorist matters. In computer-science terms, the problem is not latency but bandwidth. In lay language: if the rate at which you seize PCs exceeds the rate at which you can image, index, search and analyse the contents, then the queue just keeps on getting longer. Extending time limits is at best a measure of desperation that gives only a one-off and very short period of respite. As data volumes double every 15 months, and as more and more devices acquire processors and communications, the solution cannot be found there.
14. FIPR believes that the police need a radical improvement in forensic capabilities: more experts, and better tools. The tools also need to be usable more widely, so that investigators are not stuck waiting for specialists. This is not just a resource issue, but an issue of attitudes and priorities at the policy level. IT must come out of the 'ghetto'; a force that expects 90% of its officers to be able to drive and 30% to be qualified in firearms should not be stuck with 2 computer-literate constables. Now that IT is part of the fabric of almost all our lives, the number of computer-trained officers should logically exceed the number trained in firearms and approach the proportion able to drive.
15. It must also be realised that sometimes information just will not be found, even when it is there. This already happens with non-digital evidence; from time to time a re-examination of old case material by a fresh mind or by new methods results in a conviction where none had been possible before, or even an acquittal on appeal of someone whose conviction was unsatisfactory or even mistaken.
16. The inevitable failures of digital evidence will include failures of new kinds. For example, complexity causes new problems. Much computer science and software engineering research over the past forty years has been directed towards developing tools and techniques to cope with ever-more complicated programs and data structures. An analogy we sometimes use is 'climbing the complexity mountain' – with more and more effort one can get a little higher up, but the mountain always wins in the end. For example, it is often said that 'one-third of large software projects fail', and this seems as true now as in the 1960s. So has there been no progress in software engineering? On the contrary – we build much bigger and more expensive failures nowadays! The big project failures of the 1980s or even the 1990s might be quite manageable today. It is human nature to try to push the limits and achieve what no-one has done before, and the computer industry being young is less risk-averse than government.
17. Thus it should surprise no-one that the complexity of evidence available in some investigations and trials will exceed the analytic and management capabilities of the tools and techniques that the police have at the time. The existence of unmanageably complex cases cannot be accepted as a justification for extending the detention term, or we will end up with indefinite detention without trial.
18. Data retention is another issue that Parliament and the courts will have to tackle: should the police keep all data they have ever seen, as they have recently been doing with DNA data? There may be a case for this in terror and serious crime cases, but if data retention were to become universal for normal crime then police capabilities would be overloaded even worse than at present, and there would be serious conflicts with data protection and human rights law.

19. There are also matters of court procedure – in fact, quite fundamental issues of what it means to have a fair trial. As the quantity of material available to the prosecution and defence grows from the megabytes through the gigabytes into the terabytes and beyond, old-fashioned procedures for disclosure and discovery will become ever more inefficient and contentious. It will be increasingly easy for the prosecution to hide critical evidence in such a mass of irrelevant garbage that the defence are ambushed at trial. (I have been an expert witness in a civil matter where this happened.) Court procedure, in both criminal and civil sectors, has to be upgraded for the age of Google. This will raise many complex and difficult questions, and will no doubt have to be revisited every five to ten years as forensic and search technology both advance. I expect that such issues are beyond the remit of the committee's present inquiry, and suggest that a separate inquiry might be a suitable way forward.
20. Fundamentally the question of how long it's reasonable to keep people in jail from arrest to charge (and from charge to trial) is a political one. So is the question of what proportion of national resource is to be devoted to law enforcement and the legal system. Whatever time limits are imposed – from the wonderfully brisk 110-day rule in Scotland to the much more languid timescale considered normal in some foreign countries – police will work to these limits. Policemen, like everyone else, have conflicting claims on their resources; and if they have more time, they will take more time. They will also find cases in which (even with hard work) they cannot analyse the available data within the time limit or indeed at all. Arguments can always be made that given more time case X might have been solved. A sceptic will point out that the real limit is not usually the technology, but the attention and stamina of the human investigators. The point of diminishing returns is reached all too soon.
21. The computer industry's response to the complexity inherent in large systems may provide an instructive parallel. Successful project management requires a rather brutal approach: the manager must focus hard, close down options, parallelise the work where possible and ship a good product within the time limit set by the customer. Investigators will have to learn these skills, and find appropriate ways to develop and exercise them within a framework that gives full access to the defence, and the benefit of the doubt to the accused.
22. It is also worth remembering that how long we keep people in jail is, at a deep level, a statement about what sort of society we believe we are, and what sort of society we collectively decide – through our elected representatives – to become.
23. In conclusion, FIPR does not believe there is a sound technological argument for increasing the detention time limits. There is a strong argument, however, for supporting the police in pushing through the necessary cultural change – and acquiring the necessary budgets – to get abreast of the opportunities that digital evidence provides.

Professor Ross Anderson
Chair, FIPR
Cambridge, 27th January 2006