The Foundation for Information Policy Research

Consultation response on

‘New Powers Against Organised and Financial Crime’

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.

Response to Q1 and Q2.

We object strongly to the assumption made throughout this document, and expressed perhaps most clearly at 1.3 p 18, that consent to data sharing is irrelevant: "If vires to share exist, then consent is not needed; where vires do not exist, consent will not be a substitute."

This is completely wrong as a matter of both data protection law and human-rights law. To override a lack of consent to data sharing, the relevant law must narrowly define the purposes of processing (especially for sensitive data); under ECHR 8(2) the processing must serve a legitimate aim, and be necessary in a democratic society. A mere enabling vires provision will usually be insufficient.

Even where consent is relied on, it is not valid if the purposes are defined too broadly. Consent also may not be obtained by coercion (e.g. by the threat to withhold essential services such as healthcare or benefits).

We believe that the Government is going down the wrong path on data sharing and has been ill-advised by DCA. There is a serious risk that large sections of the public sector will come to rely on systems that are eventually found to be illegal under European law (which is also UK law), thus forcing a future government to make radical, disruptive and expensive changes in public administration.

Response to Q3 and Q4.

For these reasons, we have significant reservations about SOCA and other law-enforcement agencies obtaining wide access to public sector data. Our objection is not so much to the activities of SOCA per se as to the inevitable function creep, mission creep, and spread of access to other departments whose use of data supplied for other purposes (including sensitive data) is likely to be found illegal at some future time.

The Home Office should recall the public outcry over regulations proposed under the RIP Act which were perceived to be extending communications intelligence capabilities to many public bodies with some peripheral law enforcement function, from parish councils to the Egg Marketing Board. Ministers should ask themselves whether providing data mining powers on a similarly broad scale would (a) accord with public expectations of what privacy intrusions are reasonable (b) be found by courts to be necessary and proportionate under human rights law.

FIPR also objects to the term 'identity fraud' as being unhelpful to clear thinking. A typical 'identity fraud' consists of two linked offences, for example:

1. a criminal pretends to be a creditworthy citizen, borrows money from a bank and disappears. This is impersonation, a fraud against the bank;

2. the bank on failing to recover the money from the law-abiding citizen blackens her good name with credit reference agencies, making her life miserable for some time. This amounts to a series of offences under the Data Protection Act committed by the bank and the credit reference agency. (It is also libel but the UK rules on costs and legal aid generally preclude the citizen from obtaining relief by a libel action.)

The correct way for the Government to deal with 'identity fraud' is to encourage, empower and fund the Information Commissioner to enforce the Data Protection Act rigorously against the banks and credit reference agencies. Only then will they have the correct incentives to make the socially-optimal level of investment in authenticating new customers properly. This is not fundamentally a matter of technology, but of economics.

We believe it would be a retrograde step for the police to become even more entangled with the banking industry through CIFAS, as CIFAS has every incentive to try to dump its members' liability by rebadging impersonation as 'identity fraud'. Police units investigating bank fraud have already been criticised for being too sympathetic to the banks' viewpoint and insufficiently sympathetic to the customers'; the proposed linkup would make matters worse. At most, the government should make it easier for banks opening accounts for new customers to check whether the customer has been reported as deceased.

Response to Q5.

One of the goals of the proposed law is to enable police officers to close down phishing sites and other criminal online enterprises by telling the ISP, or other service provider, that their service is being used for nefarious purposes and that they face prosecution unless they withdraw the service. Police officers have already waved the Proceeds of Crime Act at ISPs, without being sure about whether they could make good on their threat to prosecute should the ISP not pull down the website to which the police object. The present measure should aim to regularise the business of taking down objectionable

websites; instead, however, we fear that another loosely worded Act will be added to the policeman's arsenal.

While the goals are admirable, FIPR believes that the proposed mechanism is flawed. It enables the police to threaten the good guys – the ISPs – into working with them against the bad guys, but using mechanisms that are opaque, that allocate legal risks incorrectly, will erode consumer confidence, and which may deepen the digital divide.

With the best will in the world, mistakes happen. There are many ways in which even police with specialist IT training commonly mis-identify online wrongdoers, such as misreading timestamps and thus mapping IP addresses to customers incorrectly. The recent policy decision to mainstream computer crime will leave much online enforcement in the hands of officers without specialist training or experience in computer forensics. Law-abiding customers of an ISP will thus find their service suddenly terminated because of a police threat to an ISP that may be founded on an honest mistake. All of a sudden their websites will vanish and they will receive no email; their businesses will be unable to trade.

In such circumstances it is essential that customers should be able to find out promptly why their service has failed, and should be able to challenge the decision to cut them off. These decisions must therefore be open and justiciable.

We believe the Home Office should rather emulate the 'notice and takedown' procedure currently used for copyright infringement. A police officer believing that (say) www.fipr.org was being used as a phishing site would present a takedown notice to the ISP; the ISP would contact the domain owner copying them them the notice and giving them time to respond; the domain owner could then contest the notice, whether by contacting the police directly to clear up a misunderstanding, or by legal action. This procedure has evolved over the past ten years to deal with just such situations, is robust, and is generally understood.

In some cases of phishing, the appropriate response time might be zero (for example, where a website had been hacked and taken over for a phishing expedition that might last only an hour). This does not affect the general principle. The notice should be served at once on the customer as his business is disconnected, so that he can identify and remove the phisherman's malware from his machines and get online again promptly. There must also be provision for compensation in cases where a website is wrongly shut down.

Using threats to the ISP rather than a proper notice procedure will have various unpleasant side-effects. First, although it may make things more convenient for the police, it will tempt them to take sites down without due care, increasing the number of false positives and eroding the considerable goodwill that the police currently enjoy in the ISP community. Second, it will expose ISPs to substantial legal risk – if a site is wrongly taken down its owner will be able to sue for damages (unless the law were to indemnify them, but this would be fundamentally wrong too). The predictable response by ISPs will be to write into their contracts clauses enabling them to terminate service at

any time with no reason given. Third, this will make ISPs very much more willing than at present to close down 'difficult' customers, ranging from people with mental health problems to volunteers operating facilities such as anonymous remailers (for example, to support freedom of speech in repressive countries, or Christian missions in countries with anti-conversion laws). This may deepen the digital divide, both nationally and internationally.

Furthermore, although we have set out at length the issues that arise with ISPs, exactly the same issues of false positives and consumer protection will arise in many other areas as well: companies that hire out cars, trucks, power tools or even office space may find themselves secretly pressured by the police into removing service from individuals without due process. This will have bad effects in these sectors as well. As well as deepening the digital divide, the proposed measure may thus facilitate discrimination of more traditional kinds against which the present Government has quite rightly been working.

Response to Q6.

We have serious reservations about increasing the liability of those who encourage or assist crime indirectly. We are concerned that, for example, such liability would be invoked on the margins of terrorism investigations, further alienating the Muslim community. We have recently seen the use of incitement charges against people who were thought to have downloaded unlawful images of child abuse, but on whose machines no such images had been found. There appears to be serious doubt in some cases about whether the individuals concerned had simply been the victims of credit card fraud. We therefore fear that manipulating the rules in the proposed way is likely to increase the risk of miscarriages of justice. In general, it is bad policy for people to be prosecuted for surrogate offences, or for the standards of proof to be lowered just because certain offences are the subject of press alarm.

Response to Q7 and Q8.

There is a view in some quarters that you can prevent online crime by 'taking away their computers'; orders have been made in a number of high-profile US cases preventing people from using IT or accessing the Internet.

Within the European framework, however, we think this is less likely to work. Now that so much of human life has moved online, depriving someone of Internet access is comparable to placing them under house arrest, and is likely to be seen as punitive rather than preventive. There may be some scope for ordering suspects to keep proper records and refrain from using anonymity services, but we suspect it will turn out to be more limited than the backers of this measure appear to believe.

Response to Q9.

We believe that the prosecution should not only have to inform the court of the likely impact of orders on third parties, but also inform the third parties themselves, so that they can be represented at the relevant hearings, unless there are compelling reasons to the contrary (see our response to Q5 above).

Response to Q11.

In the context of computer crimes, it is rather difficult to suspend service to a client without making him suspicious. It is hard to envisage what is proposed in other contexts. If it intended for example that a lawyer might be compelled to cease acting in his client's interests, but without informing the client? That would strike us as undermining the basis of trust in civil society, not to mention the right to legal assistance. If anyone can be compelled to cease actually providing a service, and merely pretend to be providing it, the implications are extremely wide. Because of the unpredictable but severe consequences, we advise the government strongly against taking this road.

Ross Anderson
17th October 2006