All Party Parliamentary Group on Privacy

APPG Inquiry into communications data surveillance proposals & the *Interception Modernisation Programme*

Briefing paper

24th July 2009

Prepared in association with

The Policy Engagement Network in the Information Systems and Innovation Group at the London School of Economics & Political Science

Secretariat: Privacy International, 6-8 Amwell street, London EC1R 1UQ UK.
Email: privacyint@privacy.org. Phone: +44 (0)208.123.7933
www.privacyappg.org.uk

Providing Early Warning protection for Parliament

Terms of Reference

The APPG on Privacy is enquiring into the implications of the Home Office proposals for its Interception Modernisation Programme.

On 27 April 2009 the Government published a consultation document *Protecting the Public in a Changing Communications Environment* which calls for telephone companies and internet service providers to substantially increase the amount of material they retain about their customers' internet usage and to analyse it against demands for disclosure from law enforcement and the Agencies.

The main terms of reference for the APPG work are:

- Given that Communications Service Providers (CSPs) are already compelled to retain customer data for a period of 12 months, what requiring them to collect a great deal more and to carry out preliminary analyses?
- Given the nature of the new ways in which people communicate across the Internet such as web-mail, social networking and online gaming, is it feasible to maintain the distinction between "communications data" and "intercepted content"? What are the implications for investigations and trials if intercept material remains inadmissible?
- Is it still reasonable that interception warrants are issued by the Secretary of State and that communications data disclosures are self-authorised by the organisations seeking them? Should these powers be exercised by the judiciary? Does the office of the Interception Commissioner provide a realistic safeguard against abuse? What Parliamentary oversight of the activities covered in the scheme is envisaged?
- Is the Home Office estimate of the costs of its programme at £2bn realistic and likely to be value for money?
- Given that a new and heavy financial burden is to be placed on CSPs, what will be the implications for the provision of universal Internet access throughout the United Kingdom?
- What other routes are available to the police and Agencies to investigate the threats that they argue are faced by the UK?
- What steps have been taken by the Home Office to ensure that other government departments and agencies are content with the way the scheme is intended to operate?
- What protocols have the Home Office agreed to with regard to data sharing within and outside government and what protections or procedures are available to the individual citizen or subject of the collected information to audit its content and movement between government departments and agencies or private operators?

Table of Contents

Summary 4

About the Government's Consultation 6

Challenges with the Framing of the Consultation 6

History of Interception Law 9

Current state of law 9

The Regulation of Investigatory Powers Act *10*

Communications Data Retention *11*

What is "communications data"? 12

Changes in Modes of Communications 15

Email service provision has been globalised 15

New modes of communicating 18

Current environment for law enforcement agencies 19

Technological background and implications of the new proposal 23

The Reality of DPI 27

Effectiveness of the deep packet inspection equipment 28

Safeguards 31

The Law 31

Issue of Warrants and Authorisations 33

CSP SPoCs 35

Interception of Communications Commissioner 36

Analysis 39

Is it still feasible to distinguish between content and communications data? *39*

How do we deal with the inadmissibility of Interception Material? 39

Who grants interception warrants and authorises release of communications data? 40

Is it feasible to think of the targeted collection of communications data rather than collect it in respect of everybody? 40

The need for precise language 41

Who will actually control the "DPI Black Boxes" to be installed at CSPs? 41

Encryption Issues 42

Advances in Mutual Legal Assistance 42

What answers can we give to law enforcement and intelligence agencies if we decide to deny them the levels of access they seek? 43

Other responses 45

Cost Estimates 48

Concluding Remarks 51

Appendix 1: Issues around the Admissibility of Intercept Evidence 53

Appendix 2: The Privacy Issues 60

A Chilling Effect? **61**

Summary

This briefing provides background to and analysis of the Government's declared plans in relation to the fast-changing nature of the Internet to modernise the powers available to law enforcement and the intelligence agencies. GCHQ has announced that it has an internal programme called Mastering the Internet and in April 2009 the Home Office published a document that consults on the need to provide law enforcement with further powers.

Summary of key points:

- Since the last substantive relevant item of UK legislation, the Regulation of Investigatory Powers Act, 2000, there have been many changes in who uses the Internet, for how long, with what level of technical sophistication, and in the range of services available through an Internet connection.
- There are indeed new challenges for law enforcement and the intelligence agencies but these need to be considered in the light of overall threat levels, the considerable additional surveillance resources technology has delivered since 2000, overall costs, and the arrangements for proper oversight.
- The Home Office consultation is limited to what is known as "communications data" – who called whom, when, for how long and from what location. Although much of this is already retained on a contingency basis under existing law, the Home Office now wants access to a substantially greater amount of information. Additionally, the Home Office appears to treat this information as though it is the less sensitive 'communications data', rather than considering it as content, even though gaining access to this information at the moment would involve an interception of the content of internet communications sessions. Historically there have been two entirely separate regimes for authorising access to communications data and for intercepting content. Doubt has been expressed that this framework can be maintained in the new ICT environment of web-based email, social networking, online gaming and cloud computing. Additional problems arise because, almost uniquely in the UK, intercepted content is inadmissible – it can neither be used nor referred to in court.
- It is important to determine whether the Home Office fully understands the extent to which it is recommending changes in the ways that surveillance activities are authorised, were its proposals approved. This would lead to a tipping of the balance in favour of state power and away from communications privacy rights for the

individual. In fact, the current policy environment already has quite weak privacy safeguards, and the proposals may go some way to worsening this situation.

- This Briefing discusses alternatives to the present legal structures. Communications surveillance powers in the UK do not involve judicial scrutiny. It is alone in the democratic world in making Secretaries of State responsible for interception warrants while for "communications" data authorisation is given by a senior figure in the organisation that wishes to use it in an investigation. The Briefing also considers the efficacy of the proposed oversight mechanism – the Interception Commissioner.
- A general level of concern has been expressed that the Home Office has not given adequate consideration to the practical and financial challenges of the technologies that would be used to give law enforcement agencies enhanced access to Internet traffic. The "black boxes", as they are known, that would provide 'deep packet inspection' (DPI) facilities would have to collect large amounts of traffic associated with each Internet user, discard whatever appears to be "content" but also to combine different streams of traffic so as to create further information about an individual. These boxes are supposed to be under the control of the Communications Service Provider, which implies significant new costs to them. If instead the boxes were under the control of GCHQ then the entire existing fabric of warrants, authorisations and judgments over "necessity" and "proportionality" would collapse.
- The Home Office quotes a cost of £2bn to implement its Interception Modernisation Programme but provides no detail about how this was derived. We have a substantial number of questions about what is and what is not included in their cost estimates, and from where the costs will be met.
- We are particularly concerned about the position of Communications Service Providers. It is a key aim of Government policy that there should be a universal broadband Internet service available at low cost throughout the UK. This is to be funded entirely by the same CSPs who might also be required to support the new demands from law enforcement.
- We believe that the Home Office consultation paper avoids discussion of meaningful safeguards. There is an urgent need for a comprehensive review of the UK Government's communications surveillance regime, with a particular emphasis on why the safeguards in the UK are significantly weaker than in other democratic countries.

About the Government's Consultation

During 2008 reports began to appear of an 'Interception Modernisation Programme' or IMP. According to the Home Office, the IMP is a *'cross-Government programme established to maintain our capability to obtain communications data and to support lawful interception, currently threatened by the advance of internet technologies and their increasing usage'* (italics ours).

On 27 April 2009 the British Government released a consultation document outlining its plans for *Protecting the Public in a Changing Communications Environment*[1] (hereafter the 'consultation document'). In her introduction to the document, the former Home Secretary, Jacqui Smith says: "I also know that the balance between privacy and security is a delicate one…. My intention is to find a model which […] strikes the right balance between maximising public protection and minimising intrusion into individuals' private lives."

The consultation is limited to the handling of what is known as "communications data", essentially records of who contacted whom, when, from where, in what technical circumstances and for how long, but not the *content* of what was said.

Challenges with the Framing of the Consultation

We have identified a number of immediate challenges with the framing of the consultation.

1. The exclusion of the issue of *content* from the public discussion about "the right balance" is unfortunate and unhelpful. In the first place, the debate is taking place within a wider agenda of the appropriateness of powers given to law enforcement and intelligence agencies measured against the protections they can provide and the risks of abuse. "Appropriateness" in this context means not only what law enforcement and the intelligence agencies have access to, but how warrants and authorisations are given, managed, controlled, audited, and used in court.
2. There are increasing practical difficulties within the new technologies in distinguishing communications data from content although the Home Office's proposed framework of the law is still attempting to do so. In particular the authorisations to request communications data and to intercept content are entirely separate regimes – which

[1] http://www.homeoffice.gov.uk/documents/cons-2009-communications-data?view=Binary

law enforcement agencies, Internet Services Providers, telecommunications companies and ultimately the courts have to negotiate and interpret.

3. A further related problem is that intercept evidence, content, is currently inadmissible in court. Beyond just being inadmissible, however, we may not even refer to the mere existence of the interception. Indeed the consultation document makes almost no reference to the differences between “intelligence” and “evidence” and the various applicable legal regimes.
4. The Home Office’s use of the phrase “maintain our capability” appears to be somewhat misleading. The ways in which we communicate with each other have undergone such enormous changes that it is fanciful to say that there are simple equivalents in the Internet and broader digital domain to the communications surveillance techniques used for conventional voice-based telephones. There are many new types of communication available between individuals, but nearly all of these are in forms that are very easily computer-readable and therefore capable of complex analysis by computers. The range of tools available to law enforcement to track and link activity and database content is now vast and growing all the time. The debate is thus not about maintenance of capability but trying to determine a proper balance in new circumstances.

There are serious implications from any substantial enhancement in surveillance powers and increase regulatory burdens placed upon Communications Service Providers. What is being proposed under the modernisation powers is that every communication transaction, and all forms of future transactions, would be deemed 'suspicious', worthy of later consideration by the police. This is a phase change not only in communications surveillance, but also in the power of surveillance by government itself. It also has serious ramifications for the future of communications service provision in Britain.

As the implications of this proposed policy are so vast, Parliament and the general public need the best available information on the nature of the challenges, the Home Office’s responses, and possible alternative techniques. We are very concerned that the way that the Home Office is conducting this consultation exercise and the legislation that follows will in fact minimise debate rather than enhance it. For instance, the Home Office appears unwilling to discuss the specific data types that will be collected by Communications Service Providers, and as such Parliament will be unable to discern the level of invasiveness of the proposals, and industry will be unable to determine the technological challenges and financial costs. It is essential that a public debate on these matters be well informed on technological, legal and regulatory, and financial issues.

This briefing therefore analyses the broader implications of the IMP proposal. It began through a consultation and collaboration with experts from industry, academia, and civil society organisations, conducted under the Chatham House Rule. Its purpose is to inform the policy-making process and thus provides a number of views regarding the need for policy change, rather than to posit a specific view on the nature of the IMP or to make

specific recommendations. In particular, our discussion of privacy issues is kept to a minimum, allowing others with greater expertise to raise these issues.

History of Interception Law

The interception of communications is the monitoring and scrutiny of private messages between individuals or organisations. The earliest obvious form is the reading of the mail. Though it undoubtedly occurred at much earlier dates, in the UK interception was facilitated by the monopoly position of the General Post Office (GPO), which was founded in 1660 and was a Department of State until 1969, when it became a statutory corporation with a Royal Charter. After 1869 it also had a monopoly of telegraphic services and after 1912 the monopoly extended to the telephone (with the exception of a few municipal services of which Hull is the best known). In 1981 the telecommunications aspect was spun off into British Telecom (BT). BT was privatised in 1984 and by then had also lost its monopoly. For many years interception of all kinds was carried out under the Royal Prerogative. The only oversight was via the informal "judges rules".

Interception was not put under a statutory regime until the Interception of Communications Act, 1985 (IoCA), which in turn had been prompted by the *Malone* case[2]. The European Court of Human Rights had held that the English practice of interception was insufficiently grounded in law to allow it to be justified under the European Convention on Human Rights, specifically article 8, which protects the individual against arbitrary interference by public authorities in his private or family life. But the change in the corporate status of British Telecom and the growth of other companies offering telecommunications services also meant that it was no longer feasible to rely on nods, winks, the aversion of eyes when the secret squirrel engineers arrived at the telephone exchange, and notions of "royal prerogative".

Current state of law

By the end of the 1990s IoCA needed reform and the Home Office published a consultation paper in June 1999. The two areas highlighted in that paper were the change in the telecommunications landscape and the need to find ways to deal with intercepts on private, as well as public networks.

The consultation paper led to the formulation of the Regulation of Investigatory Powers Act, 2000 (RIPA). Greater powers regarding communications data emerged in the Anti-Terrorism, Crime and Security Act of 2001.

---

[2] Malone v. Commissioner for the Metropolitan Police (no.2) [1979] 2 All ER 620

The Regulation of Investigatory Powers Act

The relevant principles within RIPA are:

- A regime for the issue of warrants for interception of the **contents** of messages. This is in RIPA Part 1 Chapter 1, sections 1-20. The Secretary of State issues the warrants. The product of interception is not admissible in legal proceedings.[3]
- A regime for the issue of authorisations for the acquisition and disclosure of **communications data**.[4] Authorisations are issued by "designated persons" within the agency or organisation seeking the communications data. Authorisations to obtain communications data must be approved by a person holding a senior office, rank or position with the relevant public authority specified by Parliament to be able to do so.[5]

RIPA contains a number of sections that seek to provide definitions of interceptions, communications data and traffic data. In light of proposed updates under the IMP agenda, we will visit these later. We will also revisit the blurring boundaries between communications content and content data in light of the practical guidance given by the Crown Prosecution Service in relation to trials where law enforcement has had the benefit of interception material but which cannot be admitted into evidence.

In the United Kingdom most powers under which the police can intrude on the private life of the citizen – by arresting them or entering their home are granted under warrants issued by judges of various levels; greater levels of intrusion require higher qualities of judicial scrutiny. Yet in the surveillance of communications, including the content but also the location information, a far lower threshold is provided. RIPA, as in IoCA, reduces the quality of judicial scrutiny by granting that power to Ministers or senior officials is a carry-over from the old notion of royal prerogative.

RIPA contains the power to issue delegated legislation to attend to the detail and one of the more important ones relevant to the current discussion is the Order (Statutory Instrument) which requires a person providing a public postal service or a public telecommunications service to provide an "interception capability"; in effect easy technical means for interception to take place once a warrant has been granted[6]. Although the "delegated legislation" route has the advantage of not bogging Parliament down with the

---

[3] RIPA section 17.

[4] RIPA Part 1 Chapter II, sections 21-25.

[5] The statutory purposes for which communications data may be accessed are listed in RIPA, Part I, Chapter II and in its associated statutory instruments: Statutory Instrument 2003 – Number 3172: http://www.opsi.gov.uk/si/si2003/uksi_20033172_en.pdf; Statutory Instrument 2005 – Number 1083: http://www.opsi.gov.uk/si/si2005/20051083.htm; Statutory Instrument 2006 – Number 1878: http://www.opsi.gov.uk/si/si2006/uksi_20061878_en.pdf

[6] SI 2002/1931 issued under s 12 RIPA

detail of how a law is implemented it has the disadvantage that the detail is then is not properly scrutinized when perhaps it should be.

Prior to RIPA, law enforcement requests for retained data were made under Data Protection legislation[7]. In addition, it was for the CSP to decide whether the law enforcement request complied with the exceptions allowed under s 29(3) DPA; if the CSP was dissatisfied, there was little that the law enforcement agency could do. (This was largely a theoretical concern, we are not aware of any significant requests that were refused). RIPA changed the authorisation process for data held by CSPs but did not alter the obligation to hold the data. Typically the period for which Communications Service Providers[8] (CSPs) hold the data it retained for its business reasons is for shorter periods than Law Enforcement (LE) wanted and lacked detail that might be helpful to investigators.

Communications Data Retention

RIPA in its original form only applies to communications data that is collected **after** the authorisation had been issued. Almost as soon as RIPA was in place the Law Enforcement agencies argued that they wanted access to what had been going on historically. The argument was that they frequently came across plots that were mature and in progress, and that it would be helpful to know who had been talking to whom so that the full scope of a conspiracy could be understood. Sometimes, it was said, there were immediate threats to public safety. Law Enforcement agencies knew that telecommunications companies retained communications data for their own purposes. These included what was necessary to charging their customers for usage and deal with related disputes - and to monitor for quality of service. Data could not be retained for any term beyond those needs.

The first move to overcome this block was in the Anti-Terrorism Crime and Security Act 2001 (ATCSA). ATCSA was rushed through Parliament in late 2001 in response to the terrorist attacks in the United States. It contained a large number of provisions covering a wide range of criminal and terrorist-related activity but Part 11 dealt with the retention of communications data. Parliament approved a voluntary code in connection with this in 2003.

From the perspective of the law enforcement agencies, the ATSCA powers still did not go far enough. That is, compliance was voluntary and CSPs were still concerned that certain aspects of what they were being asked to do conflicted with Article 8 of the European Convention on Human Rights (ECHR). This seems to require a “demonstrable case” for

---

[7] In essence via s 29(3) DPA 1998 which says that personal data is exempt from what would otherwise be non-disclosure provisions for the prevention or detection of crime, the apprehension or prosecution of offenders or the assessment of tax

[8] “Communications Service Provider” is a term which covers both telephone companies (fixed and mobile) and Internet Service Providers (ISPs)

each act of data retention in respect of particular subscribers and not allow blanket data retention "just in case".[9]

The UK Presidency of the EU in 2005[10] pushed a mandatory regime through the European Union in the form of Directive 2006/24/EC, on "the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC". The Directive was careful to note that this did not require CSPs to collect information that they do not already collect, but rather it focuses on requiring CSPs to retain specific types of information amongst those that they already manage. Since 2007, this has required telephone companies to retain specific items of communications data for a period of six months to two years, and internet service providers have their own list of specific data types to retain. The full Directive has been part of UK law since April 2009.[11]

What is "communications data"?

In their consultation paper regarding the Interception Modernisation Programme, Protecting the Public in a Changing Communications Environment the Home Office says: "Communications data is information about a communication. It does not include the content of a communication. It can show when a communication happened, where it came from and where it was going, but it cannot show what was said or written […] For a given telephone call, communications data can include the telephone numbers involved, and the time and place the call was made, but not what was said. For an e-mail it might include the e-mail address from which the message was sent, and where it was sent to, but not the content of the e-mail."

In this sense, communications data consists of:

- Traffic data – information about communications
- Service use data – which includes telephone call records, itemized billing, records of connections to the Internet
- Subscriber data – information held by CSPs about individuals such as who owns what phone number or owns a particular email account, together with their home address etc

The actual definition appears in s 21(4) of RIPA:

> In this Chapter "communications data" means any of the following—

---

[9] In *Marper v UK* in the European Court of Justice (Applications nos *30562/04 and 30566/0*) in December 2008, the Court used similar arguments in respect of the blanket retention of DNA samples.

[10] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:HTML

[11] An earlier version simply covered mobile and fixed line telephony (SI 2007/2199).

(a) any traffic data comprised in or attached to a communication (whether by the sender or otherwise) for the purposes of any postal service or telecommunication system by means of which it is being or may be transmitted;

(b) any information which includes none of the contents of a communication (apart from any information falling within paragraph (a)) and is about the use made by any person—

(i) of any postal service or telecommunications service; or

(ii) in connection with the provision to or use by any person of any telecommunications service, of any part of a telecommunication system;

(c) any information not falling within paragraph (a) or (b) that is held or obtained, in relation to persons to whom he provides the service, by a person providing a postal service or telecommunications service.

Sections 21(6) and (7) provide detail on the sub-set of communications data known as "traffic data":

(6) In this section "traffic data", in relation to any communication, means—

(a) any data identifying, or purporting to identify, any person, apparatus or location to or from which the communication is or may be transmitted,

(b) any data identifying or selecting, or purporting to identify or select, apparatus through which, or by means of which, the communication is or may be transmitted,

(c) any data comprising signals for the actuation of apparatus used for the purposes of a telecommunication system for effecting (in whole or in part) the transmission of any communication, and

(d) any data identifying the data or other data as data comprised in or attached to a particular communication,

but that expression includes data identifying a computer file or computer program access to which is obtained, or which is run, by means of the communication to the extent only that the file or program is identified by reference to the apparatus in which it is stored.

(7) In this section—

(a) references, in relation to traffic data comprising signals for the actuation of apparatus, to a telecommunication system by means of which a communication is being or may be transmitted include references to any telecommunication system in which that apparatus is comprised; and

(b) references to traffic data being attached to a communication include references to the data and the communication being logically associated with each other;

and in this section "data", in relation to a postal item, means anything written on the outside of the item.

It is these sections of RIPA that CSPs, law enforcement agencies and the courts will have to interpret. Protecting the Public in a Changing Communications Environment gives some examples in its Annex B.[12]

[12] P 32 of the consultation

Changes in Modes of Communications

Since the passage of these advanced laws for access to communications (RIPA) and the retention of communications data (ATCS and the EU Directive), if not before, the communications landscape has changed significantly, giving rise to some significant challenges to these relatively recent and advanced powers for law enforcement agencies.

Email service provision has been globalised

There are two main sorts of email in use. In the first and older method, the user's computer has a piece of software which interacts with facilities owned by their CSP and which enables the user to send and receive emails; the emails, received and sent, are stored on the user's own computer. Popular examples of software to do this are Microsoft Outlook and Outlook Express, Mozilla Thunderbird and Apple Mail.

In the past few years it become possible to forego the special software applications through the development of more advanced web browsers. Users, through the use of browsers such as Internet Explorer, Mozilla Firefox and Apple Safari and others could directly interact with a designated page on the world wide web, provide a user name and password – and can then read and create emails using a web-page and the facilities of the "web-mail" provider. The emails, unless specially saved or deleted, are held on the remote server. Well-known examples are Microsoft's Hotmail[13] and Google's Gmail[14], though there are many others.

Through these very popular services, the nature of 'email' under RIPA has changed, as has the jurisdiction of the storage as many of these email servers reside in other countries.

Protecting the Public in a Changing Communications Environment says that email traffic data includes: "routing information identifying equipment through which a communication is or has been transmitted (for example, dynamic Internet Protocol address allocation, file transfer logs and e-mail headers – to the extent that content of a communication, such as the subject line of an e-mail, is not disclosed)".

But of web-browsing it says traffic data is "web browsing information to the extent that only a host machine, server or domain is disclosed". This usually means the address but not the content of the front page of the web-site – the identity of pages within the website are "content".

---

[13] http://mail.live.com

[14] http://mail.google.com/mail/

The problem here is that in order to find out who has been communicating with whom via web-based email, the entry web-page must first be accessed, but every exploration beyond that ceases, apparently, to be communications data.

There is also the difficulty of how, at a practical level, you can extract the communications data from the content. First, CSPs tended to be responsible for the management of emails of their customers, so held the content and the logs in their keep. Second, in the case of the older type of email, it is sent across the Internet according to standard protocols so that in any one message, the routing and other "header" information always appears in the same place[15]. The one item in the header which is content – the "subject" – is also always

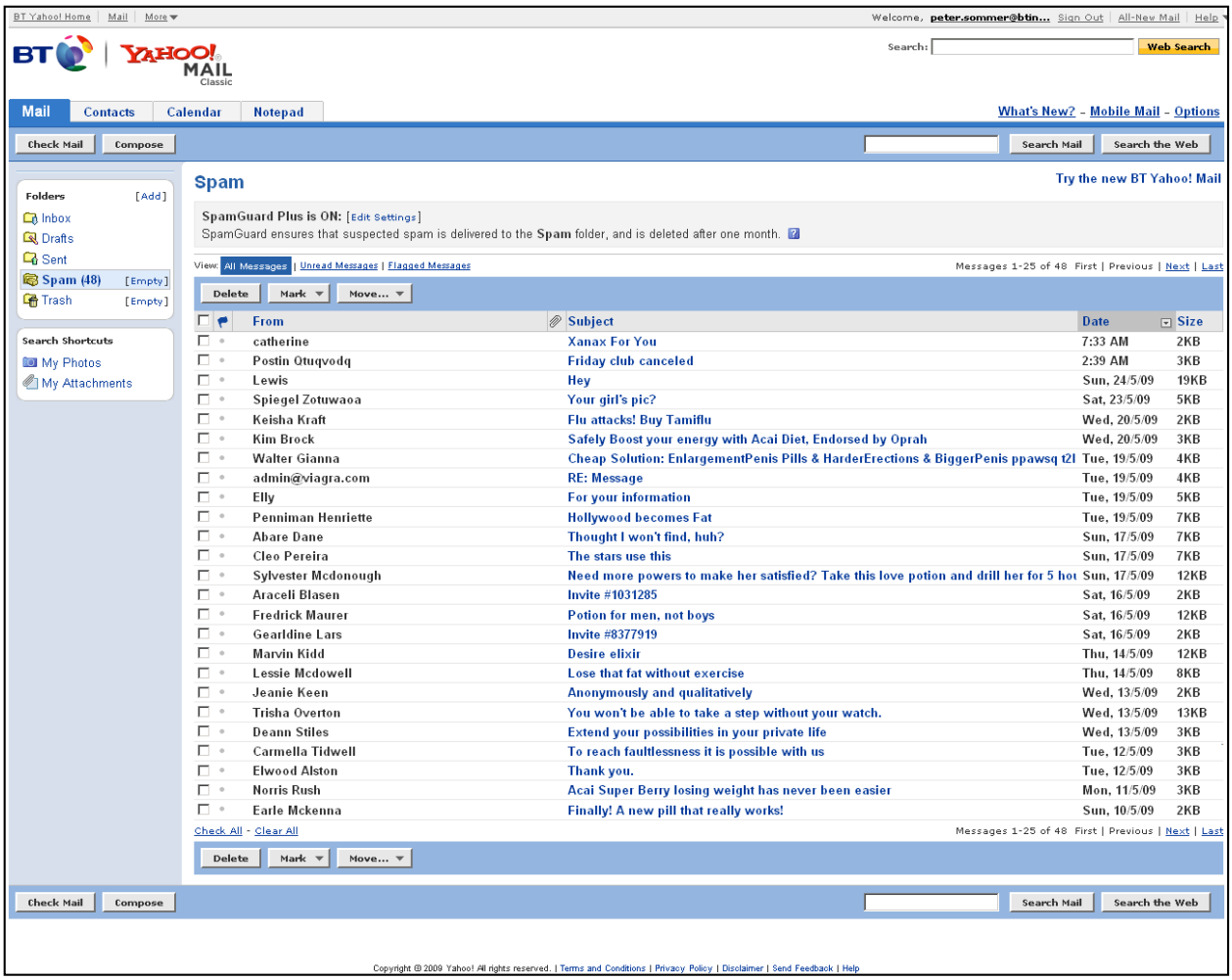
```
Form - Sun Aug 19 11:36:16 2007
X-Account-Key: account3
X-UIDL: 0MKpEa-1IMi8C3Xg6-0000RL
X-Mozilla-Status: 0011
X-Mozilla-Status2: 00000000
X-Mozilla-Keys:
Return-Path: <stuart@somesite.co.uk >
Delivery-Date: Sun, 19 Aug 2007 12:35:41 +0200
Received-SPF: none (mxeu20: 213.160.120.224 is neither permit-
ted nor denied by domain of vintagerecorders.co.uk) client-
ip=213.160.120.224; envelope-from=stuart@somesite.co.uk;
helo=ukhosts.org;
Received: from [213.160.120.224] (helo=ukhosts.org)
        by mx.kundenserver.de (node=mxeu20) with ESMTP (Neme-
sis),
        id 0MKpEa-1IMi8C3Xg6-0000RL for peter@pmsommer.com;
Sun, 19 Aug 2007 12:35:41 +0200
Received: from minime ([86.147.248.13]) by ukhosts.org with
MailEnable ESMTP; Sun, 19 Aug 2007 11:35:40 +0100
Reply-To: <stuart@vintagerecorders.co.uk>
From: "Stuart Person" <stuart@somesite.co.uk>
To: <peter@pmsommer.com>
References: <46C46ABF.2020203@pmsommer.com>
<000b01c7e019$852272a0$8f6757e0$@co.uk>
<46C474A5.8020405@pmsommer.com>
In-Reply-To: <46C474A5.8020405@pmsommer.com>
Subject: RE: Teac x-3r
Date: Sun, 19 Aug 2007 11:35:32 +0100
Organization: Vintage Recorders
Message-ID: <000e01c7e24c$abc5fe60$0351fb20$@co.uk>
X-Mailer: Microsoft Office Outlook 12.0
Thread-Index: AcfgHqJN7p59Y/xLRAO9daLXn2+H/ACLfZpg
Content-Language: en-gb
X-PhishingScore:   0
```

in the same place. As a result any competent computer programmer can write a "script" which says: take these items, discard the rest.

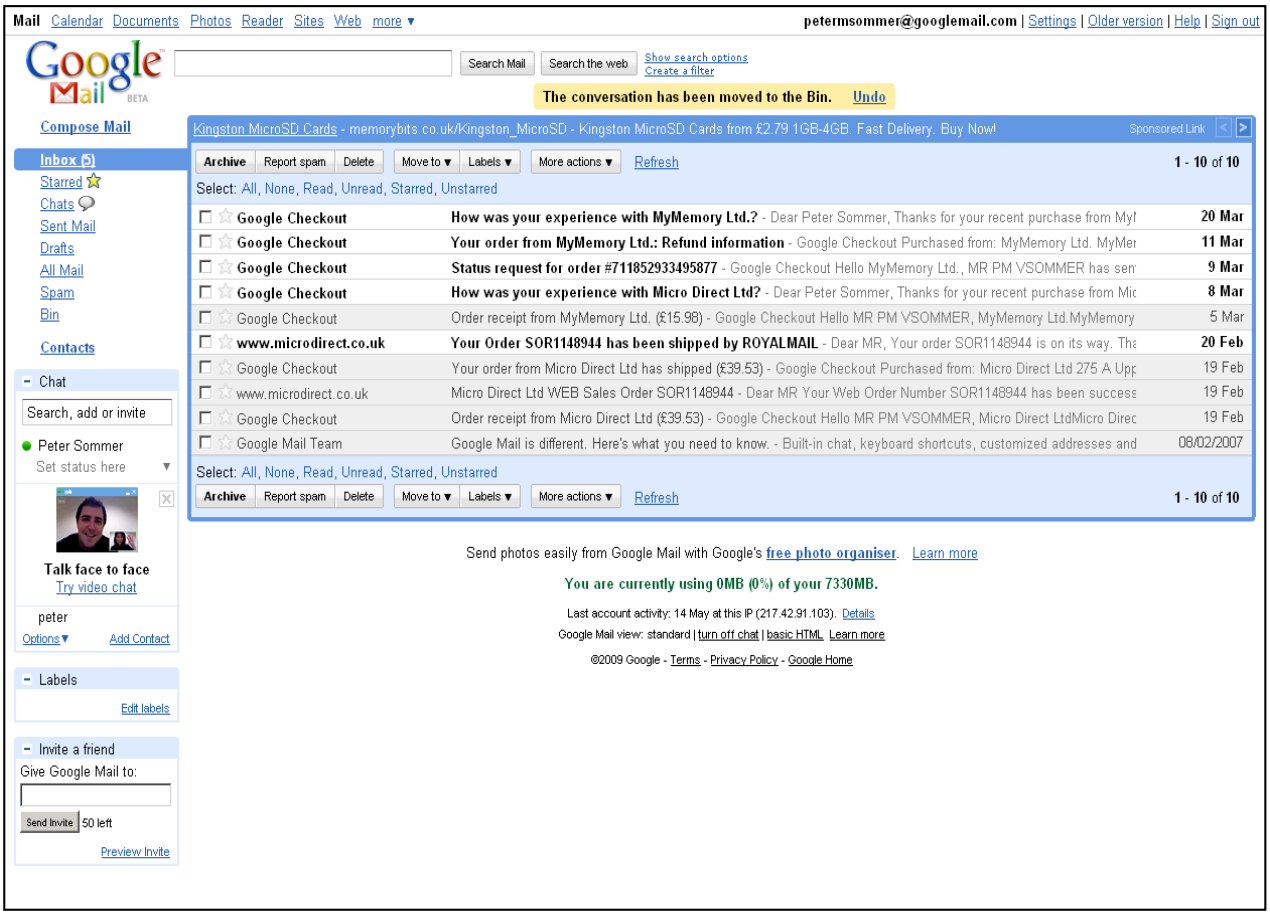
Arguably, a different script would need to be written if the communication was via a web-based email service. In fact many different scripts would be needed because there is no

[15] Most email programs routinely conceal the header of information from regular display, but it can be displayed. In Outlook Express and Windows mail (Vista), for example, you highlight the message, right-click, and then select "properties" and "details". The current standard for the syntax is RFC5322 (http://tools.ietf.org/html/rfc5322)

such standardisation. Each would appear on a website, but thereafter each web-mail supplier formats their pages differently, so that Hotmail, Gmail, Yahoo, 1&1 Internet and Exchange Server (extensively used by mid- to large- organisations) all have the relevant "communications data" in different places – surrounded by what is otherwise "content" (see below figures). Moreover, if an individual web-mail provider decides to redesign their web-pages – which many of them do in order to keep their services looking fresh – then the script to extract the communications data and discard the content will have to be re-written.



BT webmail through Yahoo!



Google's Gmail

While CSPs in the UK may very well run such services and could draft the appropriate scripts to glean the appropriate communications data, increasingly CSPs are not involved in these services and are mere conduits to service providers outside of the United Kingdom. For a CSP to access this type of information would require the gleaning of this information from communications streams, which magnifies the complexity of the surveillance practice, and again reintroduces the problem of identifying the appropriate script, i.e. is the suspect using Exchange on a mail server in Japan or Hotmail on a server in the U.S.?

New modes of communicating

Instant messaging is the ability for two users of application software to 'chat' online. While these are relatively older techniques, its use was not interpreted under RIPA or ATCS to be specifically worthy of access to or logging. Its use is widespread using relay-servers around the world, where individuals can have typed conversations, and voice and video interchanges.

Social networking sites only existed in primitive forms when communications surveillance laws were devised. On social networking sites, most often reached over the web, some of the material, including people's "biographies", photo collections, etc, is undoubtedly

"content" and only legally acquired via an interception warrant. However, people are engaging in transactions online where they are 'chatting' and establishing communications relationships including 'friendships' that are akin to communications data. There is even talk amongst experts that email is for an older age while most people communicate through social networking sites.

In online gaming such as World of Warcraft users from around the world may meet up in a virtual space to interact, discuss issues, and exchange in goods and ideas. The "communications data" would presumably include the fact that some-one had logged on to a specific service and perhaps that they had interacted with other participants – but not how they had interacted.

Each of these forms of online interaction looks different and uses different protocols. A programmer aiming at writing a "script" to separate communications data from content, if it could even be collected, would have to generate a new and separate script for each instance.

Thus, both for existing Internet-based services but for any in the future, the current separation of "communications data" from "content" looks unworkable: interpretations in individual cases are difficult; even when an interpretation is forthcoming, the practical problems of separating the one from the other are considerable. If something isn't "communications data" it is almost overwhelmingly "content" and so requires a warrant from the Secretary of State and is inadmissible in evidence.[16] This is surely not an outcome a law enforcement investigator wants.

Current environment for law enforcement agencies

It is difficult to disagree in any substance with the descriptions given in *Protecting the Public in a Changing Communications Environment* about the changing telecommunications environment; indeed one could argue that it under-estimates some of the challenges.

We can summarise them as follows:

- **Changing and multiplication of technical protocols.** In traditional telephony a direct, unique and dedicated physical link is set up between the calling parties; the role of the telephone system is to set up a unique circuit for the call via a series of switches. The circuit itself may consist of cables, radio, microwave and satellite facilities. In internet-based communications, the linking circuits are shared by a large number of simultaneous different communications; each individual communication is split into small chunks or packets, each one of which carries not only the "message" but also information identifying the originator and the intended recipient. Logical switches read the packets

[16] The CSP might have protection for their activities under s 3(3)(b) RIPA.

and send them to the right destination. The packets of data may include text, pictures, sounds, videos. It is now common for telephony to be transmitted in this packetised fashion as well – it is known as VOIP or Voice Over Internet Protocol. (Examples include SIP services and Skype). VOIP, along with other forms of Internet communication, is efficient and low cost. Internet protocols are also used to transmit high quality video; indeed there are a number of different technical protocols in existence that aim to achieve this efficiently.

- **Multiplicity of ways to communicate.** There are now many more ways to communicate. Not only do individuals make use of email and web-browsing, but we all now use many forms of instant messaging, bulletin boards, social networking facilities, file-sharing and distribution services, and voice messaging. Each one of these forms also has many individual examples, and each of these has its own technical rules – protocols – for making the communication work. Often they require their own specific client software that is installed on the user's computer or 'smartphone' like the iPhone or Blackberry. And each requires different techniques if interception is to take place – and if the communications data is to be separated and extracted. New forms of Internet communications appear all the time.
- **CSPs know less about their customers' usage.** Providers of services on the Internet keep less information about their customers. In the early days of the retail Internet when access was via dial-up, CSPs often charged by the minute – and held such information for a while in case of dispute. Internet service providers' records would show who was online at any particular occasion. But now over 90% of all connections are via broadband – ADSL or cable – which means that the link between the user and the wider Internet is almost permanently "open" even if it is not in use. The tariffs are flat-rate or may even be "free", wrapped up in media packages which include television and telephone services. The consequence is that less information is "retained" against a law enforcement request – because it is never collected in the first place.
- **CSPs do not hold information on their users in a standardised form.** Each CSP creates and holds records in ways which suit their individual business needs. The lack of standardisation means that when a law enforcement or intelligence agency receives communications data from a CSP the raw data files have to be converted into a single format. In a typical investigation investigators will need to bring together many different streams of data in order to build a picture of what has been taking place. In an emergency, it is said, events may move so rapidly that valuable time is lost while the CSPs' data is converted. In addition, in practice, some CSPs respond to requests for the supply of communications data more slowly than others. (The delay may not be the result of an unwillingness to help, but a reflection of that CSP's own computer systems and handling of its own business records).
- **Fragmentation of access and services.** In the early days of the Internet, the company that provided the user with the link to the main Internet also provided facilities for sending and receiving email and for publishing to the web. Today a typical Internet user may

additionally have a web-based email service from a third party, publish via another, download music and files from several others, and belong to various instant messaging, social networking and voice telephony services. Increasingly whole applications may be provided by a remote web-service – Google Calendar and Documents are examples of what is called "cloud computing". All of these services are run by separate companies – and many of them are likely to be outside the UK and therefore beyond the immediate jurisdiction of the UK courts. The company that provides the user with their immediate link, the ISP, will be based in the UK, but will have no reason to know or care about any of the other services their customer may be using. The ISP simply acts as a "mere conduit" for the data. The ISP does not collect any information about what their customer is doing. Indeed, as we will see, it would actually be illegal for them to do so. This is not restricted to Internet Service Providers as we have known them traditionally. The mobile phone company '3' offers users use of 3G services to make telephone calls over Skype rather than compelling their customers to use their traditional telephone networks, meaning that the log data of who is communicating with whom is actually managed by Skype rather than by 3.

- **Anonymisation.** An increasing number of services on the Internet are provided without the need for subscribers to provide accurate, or any, information about themselves to the owners of these services. This is true of many web-based email services but also file-sharing, VOIP, instant messaging and social networking. The individual users decide how much true detail about themselves they provide to those with whom they interact. Even greater levels of anonymisation are facilitated by the wide-spread availability of pay as you go (PAYG) tariffs for mobile phones which can be paid for in cash (mobile phones can access the Internet as well) and the availability of Internet cafes where online time can be purchased for cash and without the need to demonstrate identity. The wide-spread popularity of home-based wi-fi networks also allows the would-be covert user of the Internet to do so by hijacking the poorly secured Internet connection of others. Increasingly, it is difficult to identify who is behind a communication link, or how many people there may be, e.g. an entire family or community may share a single IP address, just as in the old days a number of people may have used a public payphone.
- **Greater Levels of Internationalistion.** There are now almost no inhabited parts of the world that remained unconnected to the internet and where there are, as a consequence, both consumers and service providers. An Internet service can be located within any jurisdiction.
- **Greater Volumes of Data.** Finally each year ever increasing amounts data are transmitted and received. Ofcom's 2008 *The Consumer Experience 2008 Research Report* shows that approximately 70% of the population have laptops or PCs at home and of those 93% now use Broadband. This means that 65% of adults have broadband at home. The figures from National Statistics are broadly similar. Broadband largely frees the consumer from worries about the costs of each additional usage and download. This in turn has made it possible for new services to be promoted and to flourish. Each

acts as a multiplier. In investigatory terms, more data is available to requested and captured – but then it must all be analysed.

- **Growth of "Fast Flux" techniques.** One developing trend among sophisticated cyber-criminals has been the deployment of technologies which are able to change the "internet address" (IP address) of a computer moment by moment making tracing much more difficult. In additional cybercriminals are also able to take over large numbers of innocent but poorly secured computers and herd them so that they can create remotely-controlled co-ordinated attacks. These are known as "botnets".

The task of researching the new challenges falls to GCHQ. At the beginning of May 2009 it released a press statement about an internal programme called "Mastering the Internet"[17]:

> GCHQ is heavily dependent on technology in order to execute our global missions. An increasingly rapidly changing digital world demands speedy innovation in our technical systems, allowing us to operate at internet pace, as the information age allows our targets to. One of our greatest challenges is maintaining our capability in the face of the growth in internet-based communications and voice over internet telephony. We must reinvest continuously to keep up with the methods that are used by those who threaten the UK and its interests. Just as our predecessors at Bletchley Park mastered the use of the first computers, today, partnering with industry, we need to master the use of internet technologies and skills that will enable us to keep one step ahead of the threats. **This is what mastering the internet is about.** GCHQ is not developing technology to enable the monitoring of all internet use and phone calls in Britain, or to target everyone in the UK. Similarly, GCHQ has no ambitions, expectations or plans for a database or databases to store centrally all communications data in Britain.

It is the task of legislators, experts, technologists, and lawyers to decide how and when powers of surveillance are modernised in this complex and ever-changing environment. The answer remains to be known, but it cannot possibly be as simple as the need to 'modernise' existing powers because the changes in the environment are so dramatic that a mere preservation of those powers would result in vastly different regulatory and technological regime from what we have seen before.

[17] http://www.gchq.gov.uk/prelease.html

Technological background and implications of the new proposal

From the perspective of an investigator, the best solution to the challenges of the new communications environment is to have unlimited access to the entire stream of data – upon which various analyses could be performed to recognise all the Internet protocols in place and from which to extract all the information that might be helpful. It would be even more helpful if all this data were captured and held on a contingency basis.

The Home Office consultation paper *Protecting the Public in a Changing Communications Environment* rejects this view because "The Government recognises the privacy implications in holding all communications data from the UK from a 12-month period in a single store."

If these facilities were made available, law enforcement successes would most likely increase. However such demands are really analogous to saying that were the police released from their constraints on entering private property, or to arrest and detain people[18], the levels of convictions would be much higher. The reasons for rejection are not only "privacy implications" as the Home Office document claims. The entire edifice of how warrants and authorisations are currently obtained would collapse. Instead of the situation where law enforcement, suitably legally armed, has to request/demand particular types of data from specific sources, they would have had immediate access. There would be no point at which the essential "necessity" and "proportionality" tests would be applied. It is difficult to see how any form of plausible oversight would operate. In addition, the costs to the taxpayer would be enormous. In its most extreme form every data communication within the UK would have to be stored some-where – and there would also need to be the facility to retrieve and then analyse to produce rapid results. The "Big Brother Database Machine" would have to be larger and faster than that which it was seeking to monitor – the entire UK internet infrastructure.

The Home Office also reject a "do nothing" option, leaving a so-called "Middle Way" route that it would like approved.

---

[18] The main legislation which controls this is the Police and Criminal Evidence Act, 1984 (PACE) and associated Codes of Practice

But there is very little detail about how this Middle Way which actually operate. What *Protecting the Public in a Changing Communications Environment* provides is a series of generalised aspirations.

> "Communications service providers based in the UK would […] continue to collect and retain communications data relating to their own services but **also collect and store the additional third party data crossing their networks**. This would therefore include communications data which does not come under the scope of the EU Data Retention Directive[…]. This option would resolve the problem that some communications data which may be important to public authorities will not otherwise be retained in this country. However, it would not address the problem of fragmentation: as data is increasingly held by a wider range of communications service providers, it might take longer than it does at present to piece together data from different companies relating to one person or communications device. The current capability would therefore diminish[…].To mitigate this problem the Government would require communications service providers not only to collect and store data but to organise it, matching third party data to their own data where it had features in common (for example, where it relates to the same person or to the same communications device). This would require additional legislation."[19]

The consultation paper goes on to say that the costs of CSPs/ISPs would be met, but provides no further detail.

What it means is that CSPs, in addition to their own existing systems which they need for their regular services and in addition to the "interception capability" which they must provide in order to meet the needs of law enforcement when the CSP is presented with an interception warrant[20], there has to be further equipment to carry out the collection and analysis of the third-party data ready for delivery against a valid request.

The generic name for such equipment is "Deep Packet Inspection" - DPI. In effect all this means is that the entire contents of the data stream is available for scrutiny and selections are then made on various criteria. At a trivial level DPI can be carried out using software[21] but for the large volumes and high speeds required in a surveillance situation, specialist hardware is deployed.[22] Any form of DPI is an interception under s1 RIPA and thus illegal unless covered by the appropriate warrant.

---

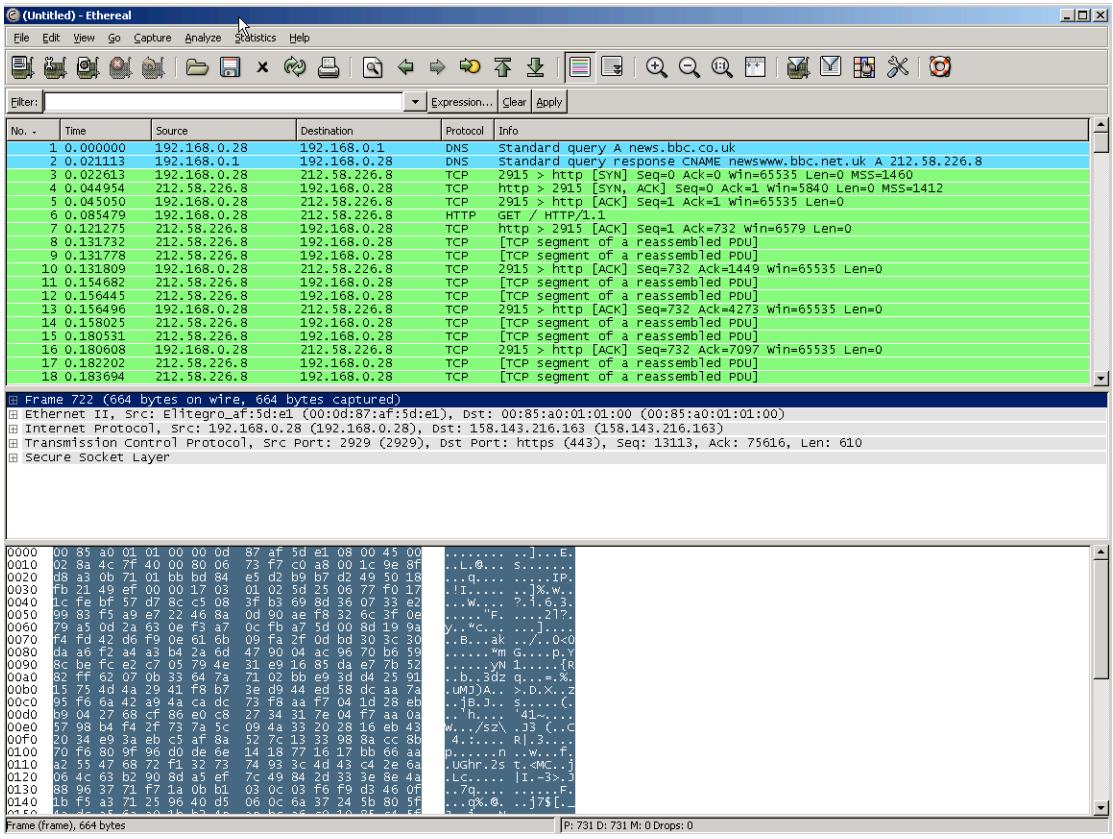
[19] Para 3.2

[20] Under s 12 RIPA the Secretary of State can "require" this.

[21] The free network protocol analyser Wireshark can perform DPI: http://www.wireshark.org/

[22] A description of some of the kit available appears in James Bamford's book *The Shadow Factory* (Doubleday, NY, 2008) at p 234 ff. – "Wiretappers"

The screen-grab below shows a DPI of an access from a domestic PC to the BBC News website.



Following from the fact that every use of DPI is in fact an interception, even though its purpose is to gain access to communications data, we see some challenging questions may arise:

- Each interception warrant and communications data authorisation must be justified on the basis of necessity and proportionality. There does not appear to be any scope for *blanket* warranting and authorisation on a contingency basis. How does this fit in with current UK and EU law? The "interception capability" currently maintained by CSPs[23] is passive; it does nothing until a warrant is received, at which point a switch is opened to feed the selected content to the appropriate law enforcement or intelligence agency facility. But the DPI kit is actively looking at the content – and the fact that the DPI kit is a machine rather than a person does not appear to make any difference in law[24].

[23] Under s 12 RIPA

[24] Consider, for example, the Court of Appeal decision in O'Shea [2004]EWHC 905.

- How is the CSP to select the third-party data which they will then collect and match? Will this be part of a legal definition or expressed in a Statutory Instrument / Code of Practice? How will we resolve differences in opinion between the CSP and law enforcement agencies as to what is included/excluded? Will any such definition be based on technical description (which would make it less ambiguous for an CSP to deploy) or on potential utility in an investigation (which would require the CSP to make judgements wholly outside their regular experience)?
- In the alternative, would there be "informal guidance" from law enforcement as to what to collect? But if so, within what legal structure? How would such a measure be debated in Parliament if it is by nature informal? What happens if, on later inspection, the courts decide that the framework within which the advice was given was in fact illegal?
- There are the practical problems of preparing and distributing the various "scripts" necessary to separate out the communications data from the content. Who is to do this, whose responsibility is that each script works, what happens if the script inadvertently releases "content"? Who funds this never-ending program of script development?

There are related problems to do with the ways in which different streams of communications data are matched and combined – and themselves combined with "subscriber information" which is information held or obtained by a CSP about persons to whom the CSP provides or has provided a communications service.[25] In the consultation paper, the Home Office say:

> "the Government recommends…. that it legislates to ensure that all data that public authorities might need, including third party data, is collected and retained by communications service providers; and that the retained data is further processed by communications service providers enabling specific requests by public authorities to be processed quickly and comprehensively."

The mechanics of this process is surprisingly vague. Assuming that it is possible and known how this can be done, the CSPs will have to decide whether this "processing" is to be carried out on a contingency basis or whether they must wait for a specific request. This again gives rise to concerns about funding as this is an onerous and continuing burden.

There is an apparent alternative route for managing DPI kit. While leaving the boxes nominally in the possession of CSPs, actual control over these boxes can be given to GCHQ, who would then provide the programs to separate communications data from content and to have in place the likely-to-be-needed data matches. Remotely programmable devices are common in the data communications world and are used to manage data switches, firewalls and anti-malware devices among others. This route would reduce both the cost and the administrative and legal burdens on the CSP. However there

[25] See p 34 of the consultation document

would be a significant risk that either communications data or content of both was released to the authorities outside the scope of a proper warrant or authorisation.

On these, as in so many other areas, *Protecting the Public in a Changing Communications Environment* is silent.

The Reality of DPI

It is important to note that what is being considered is a new form of data collection because service providers do not currently collect this information. What used to be about 'access to communications data that existed within ISPs' is now about 'collecting ephemeral data that no one currently collects', and data not collected by service providers within the UK. This policy relies intensively on Deep Packet Inspection technologies to achieve this goal.

DPI is not necessarily the panacea in this scenario that some may presume it is. As instances,

- Communications data are hard to interpret outside their operational context. It is not an easy task for an analyst to interpret them without an intimate knowledge of a service provider's network (that changes over time) or the structure of the service being used.
- DPI may be able to detect the fact that there is some form of criminal activity, but additional processes would be necessary to go after the suspects. These may include content interception or investigative work to interpret the communication data, and understand what physical or social process maps to this particular pattern or network use.
- While a large fraction of the population will be easy to identify, a significant fraction of people, particularly those involved in suspect activities and using surveillance countermeasures, will always be difficult to identify or detect.

As such, for finding and identifying the fraction of users of interest to law enforcement and what exactly they are up to, we will still need the police to do policing work. Therefore we should be mindful of the fantasy of solving crimes by merely looking at results from queries across databases.

DPI-equipment could also be used to pick apart any unencrypted protocol including instant messaging, chat rooms, and even online gaming. Challenges still exist, however.

- Internet Relay Chat (IRC) and instant messenger (IM) is relayed through a third party server, so the chat server is at the centre of the conversations. Therefore from an ISP-level, it wouldn't necessarily be possible to see that PersonA is speaking with PersonB. Rather, DPI-equipment would only identify that ISPCustomerA is in fact interacting with the IRC third party server. Additional data would have to be intelligently extracted by the 'black box', and this is more data than DPI-equipment would currently capture.

- Access to online gaming and virtual environments would be complicated. If it is known that terrorists are using Second Life to meet and plan future activities, DPI-equipment could be used to pick apart Second Life protocols to identify 'traffic data' and coordinates of users in Second Life. So if known terrorists are meeting at coordinates (x,y,z) in Second Life, then all other traffic around the UK at those coordinates in Second Life would also be monitored. But this would only be possible if the data from every Second Life user in the UK was being successfully monitored, and that police could approach each and every Communication Service Provider in Britain to piece together all of the information.
- If suspects were to collaborate together to create documents in the cloud, a commensurate surveillance regime would be to monitor who has access privileges to every document in the cloud. This would likely give rise to great concern among small and medium sized companies who tend to use these services, and to the larger service providers who stand to lose out on this business model because of the lack of confidence and greater scrutiny in their services.

In each of these cases, access to this level of data requires that the DPI-kit would be reprogrammable and could be retargeted. This is particularly true as protocols changes, and new services and protocols come into being. This will be further complicated by the use of encryption technologies.

Effectiveness of the deep packet inspection equipment

The truth is that all DPI-kit are currently built differently. As examples, the types of DPI used for online advertising are significantly different from the types of DPI that monitor the trade of copyrighted material on ISP networks. Most commercial applications using off-the-shelf DPI equipment do not need to reliably intercept every packet to prevent covert communications, and the processing they do per capture is minimal. [26]

Yet we are uncertain if the equipment for this type of system can even be built to perform all operations law enforcement expects. In effect DPI equipment is more complex than the special-purpose infrastructure equipment used to route communications. Thus DPI will always be slower and more expensive than the equipment used to route traffic, and will always struggle to keep up with the volume of information passing by, let alone the ability to process it intelligently.

When the DPI-kit will go out to tender to fulfil the needs of this proposed regime, it will probably be more of a wish list of performance and operational requirements rather than a realistic scheme that is tightly defined specified.

[26] We are aware that the Government is testing some DPI-kit with at least one major telecommunications provider and that funding is already allocated for the scheme.

If this policy were to proceed, and DPI kit would be installed in each and every ISP, would this DPI be able to deal with changes in the way people communicate, changes in the available services, and changes in the way broadband technologies operate? The answers to this question are actually quite complicated.

If the DPI kit is adaptable, then the DPI kit will be more expensive to begin with. Additionally, it will be expensive because it will have to be constantly updated. This type of technology would be on the cutting edge, where leading firms would have to be contracted to develop this form of technology, and thus we incur opportunity costs where these firms and specialists could instead be expending their time on developing more efficient and effective means of communicating. Maintaining this type of system for changes in the operating environment will in turn also require constant investment.

If the kit is not adaptable for innovations in the delivery of communications and the types of applications used, then the situation is even more complicated. That is, when ISPs upgrade their services it will render the DPI kit redundant. One way forward would involve developing and implementing new kit every time an innovation took place, which would require constant investment in DPI equipment following the innovation cycles of telecommunications equipment (that are very short). Another way would be to require ISPs to not actually innovate and update their technologies and actually restrict access to specific services and applications, in order to the DPI equipment to retain its effectiveness. This could stifle innovation and would indeed interfere with the development of a plan for 'Digital Britain'.

Already we have seen this problem arise. Under RIPA, the government paid for the first generation ‘black boxes’ within ISPs. But these 'black boxes' were designed mostly for dial-up connections. The second generation of 'black boxes', designed to deal with broadband connections, were funded by industry. The costs were significant, and it is possible that industry would be reluctant to speculatively move into a new domain of services and applications if they first had to develop a means to implement a new 'black box'.

It is technologically feasible to monitor faster and faster links, but more and more technology will be required. And monitoring links further on the edges of the network will require more and more DPI kits. That is, although DPI technologies exist, and the Government is likely to point to the availability of these technologies as a proof of concept, the reality is far more complicated. In the current applications of DPI, there is very careful attention to where the DPI-kit is placed, and not all data is captured by these devices because it is rare that all transactions need to be monitored.

For instance, even though monitoring for network security requires extensive traffic analysis, the kit designed to do the monitoring focuses on some traffic types and a large amount of the data flows, but these kits are not intended to capture all traffic. Statistical interception of a fraction of all traffic is perfectly appropriate for most commercial applications, as well as monitoring the health of networks by service providers. If the

Government's policy is to succeed, it must do what has not been done before: capture all traffic of all users. Furthermore it has to do so in real-time, and perform non trivial processing to extract communications data for a variety of applications (e.g. messaging, VoIP, etc.)

The DPI-equipment will have to monitor all traffic, pull out salient information and store this in a separate local database. The DPI-kit would have to be designed in such a way that they can be programmed remotely. For instance, a DPI-equipment like SFLOW could be used to scan broadly the traffic at an ISP, pick up occasional traffic, in order to then identify suspect traffic; the surveillance system will then focus on those specific communications flows.

All this time, however, DPI will not assist in gaining access to encrypted sessions. Although these encrypted sessions are a subset of communications sessions out there, encryption would render this surveillance regime useless unless a man-in-the-middle attack was created so that all encrypted sessions were first routed through UK service providers. Meanwhile, all the required data resides in a foreign jurisdiction in an unencrypted manner (e.g. webmail reside on the servers of U.S. companies).

Securing the configuration of these DPI interception interfaces will be a crucial challenge, since any security breach would allow for devastating attacks and illicit surveillance. This task is all the more difficult because the DPI equipment has to have the ability to be remotely upgraded, as would have to be placed outside the physical control of law enforcement agencies. Studies of interception equipment conforming to the US communications surveillance standards (under 'CALEA') were in the past found to contain multiple vulnerabilities that would allow adversaries to take them over and perform unlawful interception.

Safeguards

For online innovation to continue the government must create a regulatory environment that enhances trust and confidence, not one that generates a chilling effect on people's willingness to engage in online transactions. Greater assurances are required, for instance, over documents that reside on external servers. If the Government insists on this form of modernisation of policing powers, it must also insist on dramatically transforming the safeguards in place.

We must also devise ways to prevent abuse. The mere collection of personal information is an interference with the private life of an individual. It is difficult to implement an authorisation regime that is effective against abuse by motivated insiders. Around the world we've seen how there are politically motivated leaks of information held in secure databases, or of communications that are only supposed to be accessed under strict warrant regimes. In the UK we have seen the purposeful leaking of investigative data, traffic data of MPs, and political party membership lists; and the loss of vast amounts of personal information without clear links to organised criminal activity. The difference now is that even more information will be made available through a number of distributed databases.

Legal, procedural and technical safeguards over the use of this information can easily be changed, as we have seen the government in the past nine years change the means of communications surveillance on a number of occasions. We must therefore carefully scrutinise the Home Office's plans as outlined in their Consultation document.

The Law

Protecting the Public in a Changing Communications Environment spends some time attempting to re-assure that there are adequate safeguards. It says:[27]

> "The regulations governing access to data will continue to be separate from the regulations governing its retention. As is currently the case, public authorities will only be able to acquire communications data on a case-by-case basis from service providers under the strict regulatory framework provided under RIPA. Public authorities will only ever access a very small proportion of the data that communications service providers will continue to collect and retain and will do so primarily in the context of a criminal investigation or threat to life."

[27] p 28 of consultation document

The “strict safeguards of RIPA” would continue to be applied:

- “Data which has been retained can only be accessed by public authorities for a purpose stated in law;
- Data can only be obtained by a public authority specified in legislation, and only when authorised by a senior officer, holding a rank, office or position also specified in legislation;
- Data can only be obtained by a public authority when it is necessary in a given investigation;
- Data can only be obtained by a public authority when the interference with privacy that it will cause is proportionate;
- There is a statutory code of practice setting out how the legislation should be used and operated;
- There is external independent oversight of the application of the law; provided by the Interception of Communications Commissioner (currently Sir Paul Kennedy a former High Court judge);
- There is a right of complaint to the Investigatory Powers Tribunal if a member of the public believes that their data has been acquired unlawfully.

In addition to these safeguards, a statutory limit would be imposed on the duration for which additional data collected by communications service providers could be retained. This would relate to the data that service providers were required to collect and keep by law from services that were not offered by them, but which crossed their networks. The statutory limit would be set at 12 months, in line with the voluntary code approved under the ATCSA and in line with the UK transposition of the EU Data Retention Directive.”

The document also refers to the criminal sanctions available within the Computer Misuse Act, 1990 and the Data Protection Act and the HMG Security Policy Framework.

But as we have seen, RIPA has problems: distinguishing content from communications data turns out to be quite difficult in practice on the simple definitions so far provided – recourse to the courts for interpretation seems inevitable. Because the interception warranting process is entirely separate from the communications data authorisation process, any mistake in the latter will usually mean that content has been provided illegally. The CSP may have some protection under s 3(3)(b) RIPA, but the end product will be inadmissible. Section 17 of RIPA says:

17 Exclusion of matters from legal proceedings

(1) … no evidence shall be adduced, question asked, assertion or disclosure made or other thing done in, for the purposes of or in connection with any legal proceedings which (in any manner)—

(a) discloses, in circumstances from which its origin in anything falling within subsection (2) may be inferred, any of the contents of an intercepted communication or any related communications data; or

(b) tends (apart from any such disclosure) to suggest that anything falling within subsection (2) has or may have occurred or be going to occur.

One of the effects of this is how decisions about interception warrants and methodology can be addressed by a court. The detail of how this is handled appears in the CPS *Disclosure Manual*[28] - which acknowledges many difficult areas of judgement.[29] There are also the Attorney General's Guidelines in relation to s 18 of RIPA. [30]

The problems before a court can be surprisingly complex. As we have seen, one favoured use of communications data as evidence is to show linkages between individuals based on their patterns of "talking" to each other. The generic name for this is "link analysis"[31]. But this can be thwarted if defence lawyers can argue that the raw data has been improperly acquired or if it contains interception product that is inadmissible. Even if the link analysis is not introduced as evidence but simply used as "intelligence" it is still disclosable under the Criminal Procedure and Investigations Acts, 1996 and 2003. It is open to the prosecution to ask the court to provide a Public Interest Immunity certificate to prevent disclosure of "sensitive law enforcement methods" but there may then be counter-arguments from the defence.

Issue of Warrants and Authorisations

Interception warrants are in the hands of the Secretary of State, which for domestic surveillance is the Home Secretary of the day. The person who ends up making decisions that may have considerable technical complexity but in any event require a quasi-judicial assessment of necessity and proportionality in relation to a large-scale intrusion is determined as follows. A political party wins a majority of seats in the House of Commons on a very wide agenda of policies; internally it elects or appoints a leader who becomes Prime Minister; that person then looks among his/her colleagues and allocates cabinet posts – also on a wide agenda of policies and capabilities. The Home Secretary of the

[28] http://www.cps.gov.uk/legal/section20/chapter_a.html#148

[29] http://www.cps.gov.uk/legal/section20/chapter_e.html

[30] http://www.cps.gov.uk/legal/section20/chapter_a_annex_i.html

[31] One example of software can be seen at http://www.i2inc.com/products/

day has a considerable range of other responsibilities and there are many situations where emergencies arise; in addition such a person is a politician who from time to time will want to show the public that they are, on the one hand, tough on criminals and on the other benign to the oppressed. Decisions on the granting of interception warrants have to take place within these realities. The process has the merit of course of "democratic accountability" except that that has to take place notionally on the floor of the Commons and when not all of the relevant facts may be known. Indeed, because warrants are usually granted in great secrecy in order to avoid tipping off the target, the full facts about any one interception may not be in the public domain for several years. By that time the politician occupying the role of Home Secretary will probably have changed.

The mechanism for the issue of **Communications Data Authorisations** is described in a Code of Practice *Acquisition and Disclosure of Communications Data*[32], which is issued by the Home Office under s 71 RIPA. The power to self-authorise access to communications data is granted to the police, SOCA, HMRC, the Security Service, the Secret Intelligence Service, GCHQ and then a large number of "additional relevant public authorities who are identified in a number of Statutory Instruments[33]. In 2008 there were, for example, 474 local authorities who were approved and 110 other bodies such as the Independent Police Complaints Commission, Charity Commission, Royal Mail and the Medicines & Healthcare Products Regulatory Agency (MHPRA). [34] In each instance the authorisation is given a by a "designated person" within the organisation seeking the communications data. From time to time the Home Secretary may also qualify a "designated person"[35]. In local authorities, for example, this could be a Assistant Chief Officer or Assistant Head of Service – they are then referred to as the Senior Responsible Officer – SRO.

Again now seems a good time to question whether a senior official in an organisation with an interest in the outcome of an investigation is the best person to judge the application for access to communications data made by a junior figure in the same organisation. Increasingly the tests of necessity and proportionality will require an understanding and assessment of the technological facilities for analysis available to the investigator. It is essential to recall that what has changed is the quantity and extent of the data, as well as the ability to link several different streams of data plus information held on databases. The judgements that have to be made are increasingly complex. It remains to be known whether an "Assistant Head of Service" within a local authority, for example, has the

---

[32] http://security.homeoffice.gov.uk/ripa/publication-search/ripa-cop/acquisition-disclosure-cop.pdf?view=Binary

[33] Regulation of Investigatory Powers (Communications Data) Order 2003 and the Regulation of Investigatory Powers (Communications Data) (Amendment) Order 2005, the Regulation of Investigatory Powers)Communications Data) (Additional Functions and Amendment) Order 2006and any similar future
orders made under section 25 of the Act.

[34] Report of the Interception if Communications Commissioner for 2007; http://www.official-documents.gov.uk/document/hc0708/hc09/0947/0947.pdf

[35] RIPA s 25 (2) and (3).

necessary knowledge and skill to perform this task. We are worried that this question has never been asked under the older regime and appears to not be one of the key questions asked by the Home Office as we consider this new regime.

CSP SPoCs

The main control on the ways in which the SROs authorise surveillance is that they are required to record their decisions[36] and the reaction of the CSP employee who receives it. This person is known as the SPoC - Single Point of Contact. [37] It is worth quoting from the *Code* at this point to illustrate the issues that have to be assessed:

> The SPoC should be in a position to:
>
> - engage proactively with applicants to develop strategies to obtain communications data and use it effectively in support of operations or investigations;
> - assess whether the acquisition of specific communications data from a CSP is reasonably practical or whether the specific data required is inextricably linked to other data
> - advise applicants on the most appropriate methodology for acquisition of data where the data sought engages a number of CSPs;
> - advise applicants and designated persons on the interpretation of the Act, particularly whether an authorisation or notice is appropriate;
> - provide assurance to designated persons that authorisations and notices are lawful under the Act and free from errors;
> - provide assurance to CSPs that authorisations and notices are authentic and lawful;
> - assess whether communications data disclosed by a CSP in response to a notice fulfils the requirement of the notice;
> - assess whether communications data obtained by means of an authorisation fulfils the requirement of the authorisation;
> - assess any cost and resource implications to both the public authority and the CSP of data requirements.

We should at this stage draw attention to the extent to which some of these facilities are not being operated directly by SROs in the relationships with SpoCs, but are apparently

---

[36] Code of Practice *Acquisition and Disclosure of Communications Data;* Chapter 3 *passim*

[37] ibid 3.15-3.2o

outsourced via company called SinglePoint Data Services[38]. This company may offer administrative convenience and technical knowledge but we question whether important decisions involving intrusive surveillance should ever be delegated away from those legally charged with exercising them.

Interception of Communications Commissioner

Oversight of the processes of both interception and communications data fall mostly on an official called the Interception of Communications Commissioner.[39] Data protection issues are within the remit of the Information Commissioner. The Interception Commissioner, described as "independent", is appointed by the Prime Minister of the day.[40] His reports go the Prime Minister and are then "presented" to Parliament.[41] These Reports are published each year. The most recent is for 2007 and was published in July 2008.[42] The current Commissioner, Sir Paul Kennedy, is a former senior judge, as is often the case.

The current Report describes in some detail how the Commissioner scrutinises interception warrants – he visits the Security Service, Secret Intelligence Service, GCHQ, SOCA and the parts of the police that make most use of interception warrants and reviews a sample of warrants and all their associated files. During 2007 he also visited ten CSPs to gain an insight into their work, though these were not formal inspections.[43]. In 2007 1881 interception warrants were issued by the Home Secretary of which 929 were in force on 31 December 2007.

The Report also explains the scrutiny of communications data authorisations. There are of course many more requests of communications data than there are for intercept warrants. The Report says that during 2007 there were 519,260 such requests. There is no breakdown except that the Commissioner says that most were from the police and the Agencies. Only 1707 came from local authorities and these were usually related to trading standards and environmental health.

During 2008 there were a number of reports about local authority abuse of RIPA powers where their exercise did not appear to be necessary or appropriate, for example in relation

---

[38] http://www.singlepoint-dataservices.co.uk/

[39] There is another Commissioner in this arena – the Surveillance Commissioner. His office deals with covert human surveillance under the Police Act 1997 as well as RIPA . The specific forms of surveillance covered include "intrusive surveillance", "directed surveillance, the use of "Covert Human Intelligence Sources" (CHIS) and "interference with property". The latter includes the use of bugs, covert entry into a suspect's computer and material which is subject to legal privilege and some journalistic material.

[40] s 57 RIPA

[41] s 58 RIPA

[42] http://www.official-documents.gov.uk/document/hc0708/hc09/0947/0947.pdf

[43] 2007 Report, paragraph 2.4

to alleged fraudulent applications for school places[44]. This prompted the Home Secretary to consult on a review of RIPA powers[45] - this is a separate and current exercise.

We must therefore raise the question: is an Interception Commissioner is a plausible safeguard? As a public figure he is all but invisible – that may be the result of the tradition that judges don't give interviews. However the contrast with the Information Commissioner – whose remit is data protection and freedom of information – is stark. All the holders of that office (and its predecessor the Data Protection Commissioner) have appeared regularly at conferences and given extended interviews. They have expressed views at variance with the government of the day. Again, as a comparison with the Information Commissioner, the Interception Commissioner produces no budget or accounts for public review.[46]

There are two sorts of scrutiny that an Interception Commissioner can carry out: of process and of judgement. The first is by far the easier: it is essentially an audit exercise to see that all the procedures have been carried out. For that there needs to be documentation of the warrant or the authorisation and of the activities that were carried out in consequence, together with the records – the intercepts or the communications data that were produced. The second is to examine the judgements made when the issue of the warrant or authorisation took place; in other words, how the Home Secretary or SRO decided that the scope of the warrant or authorisation was "necessary" and "proportionate". The first is more akin to a judicial review and one can understand that a former senior judge would be much more at home with that process. Plainly any assessment of the circumstances behind the scope of a warrant or authorisation would have to be on the basis of information available at the time and not on hindsight.

Little is known about the resources available to him to assist the Commissioner's work. His Report speaks of a small secretariat and having an inspectorate. How many inspectors are there, what skills and experience do they possess? Are there enough to cope with the average of 1422 communications authorisations that occurred every day during 2007 (including week-ends and bank holidays)? Moreover, with the changes in the communications environment as described by both us and the Home Office, the Commissioner must possess considerable technical knowledge of Internet records and protocols, and also of the consequences of the latest link analysis techniques available to intelligence analysts. The annual reports provide insufficient information for us to make such an assessment as to the Commissioner's competency.

---

[44] http://www.theregister.co.uk/2008/04/11/poole_council_ripa/

[45] http://www.homeoffice.gov.uk/documents/cons-2009-ripa?view=Binary

[46] The ICO's Annual Report for 2007/08 is at:
http://www.ico.gov.uk/upload/documents/library/corporate/detailed_specialist_guides/annual_report_2007_08.pdf

By contrast we do know quite a bit about the Information Commissioner. Holders of that office appear frequently in public both to explain and debate the role. We know something of its staff – there are currently 276 of them and the budget is £16.9m. There is at least the basis for developing public trust that the job is being done, and in so far as it isn't, it is relatively easy to make evidence-based criticism. But we also know that the lack of detailed technological expertise exists within this body as well.

The Interception Commissioner's work is in turn said to be subject to scrutiny by a body called the Investigatory Powers Tribunal. This is set up under s 65 of RIPA. It has a website[47] and its remit includes all the powers given under RIPA and it can also investigate any alleged conduct by the Security Service, the Secret Intelligence Service and GCHQ. The Tribunal is essentially a body of lawyers; it currently has seven members, all senior lawyers. They do not have obvious access to technical expertise in relation to the technologies of surveillance or the ways in which such raw material may subsequently be used. It says of itself:

> The Tribunal is not able to provide information on request. Its function is to consider that any conduct covered by RIPA has been properly authorised and carried out in accordance with appropriate guidelines. It can not give a "yes or no" answer as to whether a person is under surveillance or the subject of intelligence targeting.
>
> If you want to see any information that is held on you by a particular organisation, you should make a Subject Access Request (SAR) to that organisation under the Data Protection Act. If this is not successful, you may be able to appeal to the Information Tribunal. SARs can be made to the Tribunal as well.

The Tribunal is explicitly excluded from Freedom of Information legislation. Its website currently lists four rulings.

[47] http://www.ipt-uk.com/

Analysis

It is unsatisfactory to assert that the debate on IMP should centre solely on "maintaining" capabilities for acquiring communications data. The ICT environment has changed so much since 2000 that we ought to be asking ourselves about the appropriate balance between powers given to law enforcement and the Agencies and the privacy of the individual. In addition during this same period a number of other forms of surveillance have become available to the authorities in the fight against crime, of which the network of cameras able to read vehicle registration number plates, provide instant detail of ownership (ANPR) and offer real-time movement tracking is simply one stark example. In this paper we are not trying to describe what for us would be the "appropriate balance" but to set out the issues for the public to consider.

Is it still feasible to distinguish between content and communications data?

Large numbers of requests for what might be considered authorisations "communications data" would need to be converted into requests for "intercepts". The two regimes are quite separate. As the product of interception is currently inadmissible a number of new problems for investigators and prosecutors about what they can use in evidence and what they are required to disclose under CPIA[48] arise.

How do we deal with the inadmissibility of Interception Material?

Following on from this, are these issues alone sufficient to remove the "inadmissibility of content" requirements from S 17 RIPA? The Chilcot Committee operating under Privy Council terms is looking to adjust the scope of s 17, but appears to be pessimistic that it can do so.[49] But the furthest the Committee seem to have gone is to say that perhaps in a limited number of circumstances, where it favours the prosecution, intercept evidence should be allowed. The argument we make is that it will have to be allowed in all circumstances, though with the opportunity for prosecutors to seek to exclude sensitive material on the same Public Interest Immunity grounds that are already available to protect sensitive human intelligence sources and other techniques such as the precise methods used to carry out audio and video bugging[50].

---

[48] Criminal Procedure and Investigations Acts, 1996 and 203

[49] http://www.official-documents.gov.uk/document/cm73/7324/7324.pdf and http://www.publications.parliament.uk/pa/cm200809/cmhansrd/cm090212/wmstext/90212m0007.htm

[50] See Appendix 1 for more on s17 RIPA

Who grants interception warrants and authorises release of communications data?

Is there still a case for maintaining the dominating role of the Home Secretary of the day in granting interception warrants? On the 2007 figures from the Interception Commissioner, there is an average of over 5 interception warrants are granted each day of the year – and all of them should require careful scrutiny.

Many stakeholders are yet to be persuaded about allowing SROs within the organisation to authorise release of communications data to investigations being carried out by their colleagues. We have sought to show that both of these roles are a function of history, in effect a carry-over from the notion of "royal prerogative". None of the people involved have any judicial experience, do not appear to have any significant training or technical knowledge to assist in discharging the role and have such a range of other duties that it is questionable that they will always have the time to apply their minds to the immediate problems of a warrant or authorisation at the time when they are approached to issue one. Is there not a compelling case for passing the task over to the judiciary, who exercise these powers in almost every other sphere of potential intrusion into private life? "Lesser" intrusions would go before a magistrate or district judge; deeper intrusions would go to a Crown Court judge. A "lesser" intrusion might correspond to what is in today's "communications data" requests regarding who is calling whom, but any other sort of request, because of the extent to which content will have to be probed and because of the opportunities for linking separate streams of evidence, may have to counter as a "deeper" intrusion We recognise that warrants and the like will have to be issued in secret in order to avoid tipping off suspects.

Is it feasible to think of the targeted collection of communications data rather than collect it in respect of everybody?

At the moment CSPs retain communications data in respect of all of their customers – and this would not change under the Home Office proposals. One suggestion is that some selection of customers should be made; in effect that there would be a new class of request – for communications data to be held on a contingency basis. The CSP would be told the identity of the targeted person and would retain their communications data – however that data would only be released if there were a further request/authorisation. This approach is consistent with the international standard established in the Council of Europe Cybercrime Convention.[51] This approach has some promising features, as well as some benefits from the perspective of costs. The problem is defining the criteria under which this new class of request would be issued. By definition it could only be on the vaguest of suspicions – otherwise there would be justification for actual immediate provision of communications data. There is then the potential that people complain that

[51] Council of Europe Convention on Cybercrime, ETS 185, November 2001, available at http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

they have been placed on a watch list on entirely trivial grounds – writing a letter to a local paper asking for improved traffic control facilities outside a school, for example. But our current situation is such that every citizen of the United Kingdom is on such a 'watchlist' and his or her communications are being preserved *en masse*.

The need for precise language

The Home Office consultation document, *Protecting the Public in a Changing Communications Environment*, deals in generalisations and aspirations, but for the law to work effectively and unambiguously, any proposed statue or code of practice has to be available for careful scrutiny to see that it will perform as expected and have no unintended consequences. As we have tried to show, the current definitions of "communications data" present considerable problems of practical interpretation.

It is also not enough to rely on the goodwill of law enforcement and the agencies to interpret vague laws in a benevolent fashion. The police and agencies are asked to protect the public on what they see as slender resources and it is only natural that they will seek to use as much as they can of the powers Parliament gives them.[52] The Police and Criminal Evidence Act, 1984 (PACE) was introduced because it was recognised that informal understandings about police powers were inadequate to deal with "noble cause" abuse.

Who will actually control the "DPI Black Boxes" to be installed at CSPs?

These are the boxes that are supposed to filter the entire data stream fed to all of the CSP's customers, extract the "communications data" element for retention for 12 months while rejecting the content. Additionally either the black box or some other facility owned by the CSP has to perform an element of data-matching so that, for example, when a CSP customer accesses the world wide web to visit third-party web-based email services, VOIP services and social networking sites, there is an instant linkage available to anyone who presents a valid communications data request. The legal framework says that all this data is held – "retained" - by the CSP until the request arrives. But how does the CSP know what should be retained and matched? Who produces the many scripts or routines necessary to tell the computers what to retain? Will GCHQ have access to the black boxes and if so, with what safeguards to ensure against abuse or malicious attacks from other parties?

---

[52] A striking example of this is the deployment of s 44 Terrorism Act 2000 which allows officers in uniform to stop and search persons and vehicles within a declared designated area. There is no requirement to have any reasonable grounds to conduct the search. The whole of London had been declared as such an area despite the fact that many parts of London do not contain sensitive targets. The police had acted legally, but probably not in the way Parliament intended. There have been similar complaints about the police approach to amateur photographers and handling some public order offences.

Encryption Issues

A frequently-articulated concern of law enforcement agencies is the proliferation of high-strength encryption systems. In response to this RIPA Part III contains powers under it is a criminal offence wilfully to withhold the means of decrypting encrypted material.[53] It seems to be generally acknowledged that encryption has not so far been deployed by criminals and others in UK to the extent forecast in 1999 when RIPA was before Parliament. However there has been some use.[54]

This however has been where computers have been found with encrypted material on them. Encryption can be and is of course used for data in transmission. The simple use of a secure web browsing session, for instance, would undo any attempts to gain access to web-mail communications data. Depending on how precisely this is done, the current proposals, or any others that can readily be visualised, would appear to have no answer. And to that extent any investment runs the risk of being wasted.

Advances in Mutual Legal Assistance

In the case of the problem of offshore communications, i.e. people are using foreign mail providers it is not as easy for governments to gain access to emails, unless it is in a real-time manner, from what we can understand, many of the key providers are very good at responding to foreign government requests. The main mechanisms for formal international legal co-operation are the Mutual Legal Assistance Treaties (MLATs). For those that have signed up, the Council of Europe Cybercrime Convention [55] is an important advance in that it seeks to harmonise definitions of cybercrime and methods of obtaining evidence across borders particularly in cases where two countries are lacking a MLAT. Anecdotal indications are that co-operation is at its best when individual officers in different countries already know each other; some crimes, such as those involving the sexual abuse of children, get much better qualities of co-operation than, for example, fraud. There are international law enforcement organisations such as Interpol[56] and Europol.[57] An important policy aim must be to improve these mechanisms.

---

[53] RIPA s 49. The details are spelt out in a Code of Practice: http://security.homeoffice.gov.uk/ripa/publication-search/ripa-cop/electronic-information?view=Binary

[54] For example in an “animal rights” case: http://www.out-law.com/page-8634

[55] http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm

[56] http://www.interpol.int/Public/TechnologyCrime/default.asp

[57] http://www.europol.europa.eu/publications/Serious_Crime_Overviews/HTCThreatAssessment2007.pdf

What answers can we give to law enforcement and intelligence agencies if we decide to deny them the levels of access they seek?

The position of the Law Enforcement agencies is quite clear and is reflected in the quotation in the Home Office document by a quotation from Stephen Lander, the former Director-General of the Security Service who is now the current Chair of SOCA:

> "Any significant reduction in the capability of law enforcement agencies to acquire and exploit intercept intelligence and evidential communications data would lead to more unsolved murders, more firearms on our streets, more successful robberies, more unresolved kidnaps, more harm from the use of class A drugs, more illegal immigration and more unsolved serious crime overall."

But the law enforcement agencies *never* have all the powers they would like. As a society we restrict such powers because of cost, risk of abuse, threat to privacy and because, in the end we make a risk judgement. That judgement is that we will put up with a certain amount of unsolved and unprosecuted crime because the alternatives in terms of the costs of more law enforcement resources and powers become unacceptable.[58]

What is also true is that, far from diminishing, the facilities to track people electronically have show considerable expansion. In addition to the many new sources of communications data logging which can be requested and the availability of location data to show where people have moved around, there are also considerable analytic facilities which allow all this data to be aggregated.[59]

Beyond this, it is also useful to remember that overall crime in the UK is showing a downward trend. These two charts come from the most recent Home office-sponsored and published *British Crime Survey*:[60]

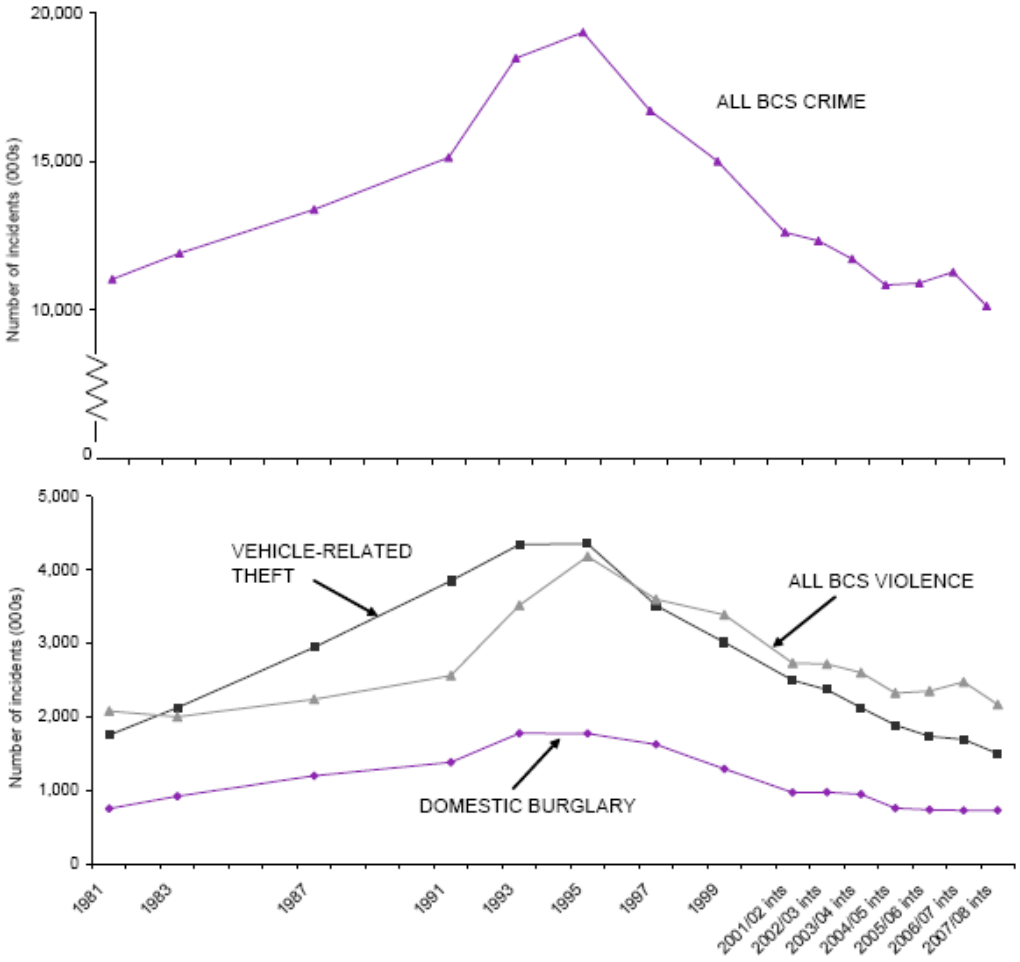
---

[58] In their report *Could 7/7 Have been Prevented?* the Intelligence and Security Committee say: " We have already explained that MI5 would have to be unacceptably large if they were to provide full coverage": http://www.cabinetoffice.gov.uk/media/210852/20090519_77review.pdf

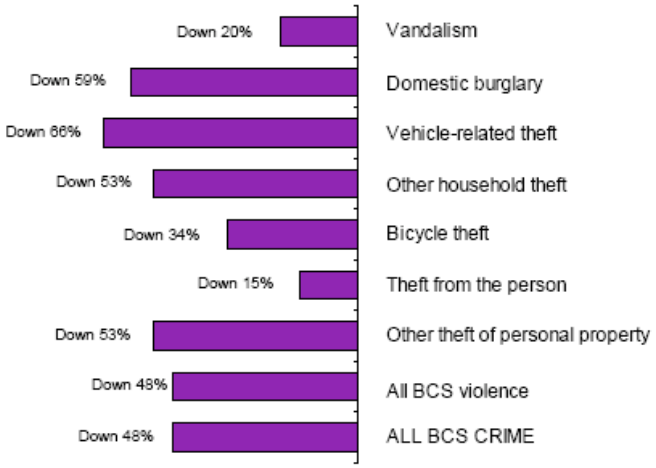
[59] See also the analysis in the *Database State* report from the Joseph Rowntree Reform Trust: http://www.jrrt.org.uk/uploads/Database%20State.pdf

[60] http://www.homeoffice.gov.uk/rds/pdfs08/hosb0708.pdf. One further additional finding is that two out of three people *perceive* crime as increasing nation ally, though only 40% of the public thinks this is true in their own area.

Trends in crime, 1981 to 2007/08 BCS



Percentage change in BCS offences, 1995 to 2007/08



It is also worth recording the actual numbers of people in the UK who have died in terrorist incidents as the spectre of terrorism is so frequently raised in discussions about the need for more surveillance. 52 people died in the London attacks of 7 July 2005; 29 in the Omagh bombing of 15 August 1988 and 21 in the Birmingham bombing in 1974. The largest single loss was 270 lives at Lockerbie in 1988, but there the target was almost certainly not the UK. Each year nearly 3000 people die in road traffic accidents. If we take the worst recent year of 2005, when "7/7" occurred, there were 3.200 road deaths[61] and 3774 deaths from accidents in the home[62], so that you were over 61 times more likely to die in a road crash and 72 times more likely to incur a fatality in the home than to be killed in a terrorist atrocity

A further concern is that the police and agencies are not making the best use of the intelligence already available to them. In their 2009 report *Could 7/7 Have been Prevented?* the Intelligence and Security Committee say:[63]

> "There tends to be an assumption, fuelled by their portrayal in the media and fiction, that MI5 can access any information from any database in an instant. We know this is not the case but nevertheless, as the Head of MI5 acknowledges above, their record keeping is not as good as it should be. In 2006, MI5 began a significant investment programme (called "information exploitation") that will address some of these issues and should improve the way that intelligence is brought together, stored and analysed. This will help investigators to analyse large quantities of data covering a significant number of targets. It enables investigators to better identify targets and their associates from fragmentary information, analyse their activities, establish connections between people and will help to focus limited resources. We believe that this new programme will provide a substantial improvement in MI5's ability to make the most of the intelligence that they gather, and hope also to see a general improvement in their record keeping (and consequently in their ability to provide a clear audit trail)."

We therefore must ensure that our law enforcement officials are trained and aware of their existing powers before we expand their powers dramatically.

Other responses

There are other items in this agenda that we should also be including before reaching any conclusions about the current "best balance". For example:

---

[61] http://www.statistics.gov.uk/downloads/theme_social/Social_Trends37/Social_Trends_37.pdf, p 167

[62] http://www.statistics.gov.uk/downloads/theme_health/DH4_30/DH4_no_30.pdf

[63] http://www.cabinetoffice.gov.uk/media/210852/20090519_77review.pdf, paragraph 171

- **Anonymous telephone and Internet facilities.** The biggest single restriction in tracking individuals is the continued availability of pay as you go (payg) mobile phones. These can be easily legitimately purchased for cash without any need to provide personal data. For the less-than-£5 per SIM the criminal or terrorist is able to keep anonymous contact with his co-conspirators, surf the internet from a smartphone or netbook and even have the means to detonate an improvised explosive device. There are now 122.6 active mobile connections per 100 of the population.[64] Two-thirds of all mobile contracts are pre-pay, as opposed to based on monthly contracts.[65] We can say with great certainty that any proposal to force all UK mobile phone subscribers on to monthly subscriptions would be robustly attacked by both the mobile phone providers and their customers. But the issue here is the same as for seeking increased powers to access regular communications data – how big is the threat and how far are we prepared to make sacrifices in order to be "safer"? Similar arguments could be made about the use of Internet facilities in cafes and libraries where the only credential required is the ability to pay a small fee or buy a cup of coffee. There would be no cost to the taxpayer in the necessary legal changes to make all mobile phone contracts monthly and subject to identity checks. As with the laws on the possession and sale of guns, the effect would be to make life more difficult for the criminal and terrorist; plainly 'anonymous' phoning and Internet use would still continue for the determined.
- **Police Training in ICT investigations.** There is an urgent need to see that all detectives understand the new ICT environment. Some 70% of the UK population enjoys Internet at home, 90% of those by broadband. Because of the speed of change in the ICT landscape it is not enough that each detective is given a basic "awareness" training; frequent updates are necessary as well. There is little point in giving the police increased powers to acquire communications data if, throughout the country, individual police officers don't know how to make best use of what is available to them. The matter goes further: collecting communications data is only one aspect of the amount of digital evidence potentially available in any investigation. In terms of what can be presented in court and linked to specific individuals, personal computers are hugely significant. They often carry the digital footprints of any individual over several years – their web-browsing, their emails, the documents and pictures they have downloaded and shared. At the moment UK law enforcement has about 300 police officers in formal High-Tech Crime Units and employs overall between 500-600 specialist computer forensic examiners, both police officers and civilian employees.(The two figures overlap) In most police forces there are backlogs in excess of six months for "non-urgent" (i.e. where there is no immediate threat to life or serious conspiracy in progress) examinations.

---

[64] http://www.ofcom.org.uk/research/cm/cmr08/telecoms/

[65] http://www.ofcom.org.uk/consult/condocs/msa08/msa.pdf paragraph 3.23

- **Prosecution Training.** Similar arguments must apply to the capability of the Crown Prosecution Service to mount prosecutions based on these classes of evidence. We understand that to date only 120 prosecutors have had high tech crime formal training.

Cost Estimates

Protecting the Public in a Changing Communications Environment says: "Initial estimates of the implementation costs of the range of options discussed above are up to £2bn. This figure is a high level budgetary estimate of the economic costs". This obviously excludes the Home Office's "do nothing" option.

There is no explanation or detail of how these costs are derived. Pausing briefly to wonder about the distinction between "costs" and "economic costs", is this simply the cost to the tax payer in terms of facility fees that might have to be paid to CSPs? Does it include the new "DPI" hardware? What about including the transitional infrastructure costs likely to be incurred by CSPs as they convert their existing systems to produce records into formats more helpful to law enforcement? Does it also include the costs to CSPs of additional SpoC staff and/or further training for existing SpoCs as they range and complexity of requests is likely to increase? What about the cost to CSPs of the data matching the paper mentions? Does the figure include the additional costs to be borne by those requesting communications data – again they will need further training if their requests are to meet the "necessity" and "proportionality" tests in the more complex ICT environment? By the same token, does the estimate include the additional costs to law enforcement and the agencies so that they can take advantage of the new material available to them? We have also seen that the DPI hardware will need a program of on-going development, to respond to new Internet-based services.

We need detailed costings for three main reasons:

1. The UK government is inconsistent in its ability to implement complex computer systems. In addition to soaring costs of NfIT, now said to be projected at £12.7bn[66] we can point to the failure of SCOPE[67], promoted as a secure computer network providing key officials with speedy access to secret intelligence on terrorism and other threats, development of which was frozen in July 2008.[68]

2. Policy makers need to gauge investment against benefit in this arena as elsewhere. We can call this the "helicopter" test. Helicopters have undoubted benefits to police

[66] http://www.publications.parliament.uk/pa/cm200607/cmselect/cmpubacc/390/390.pdf; http://www.publications.parliament.uk/pa/cm200809/cmselect/cmpubacc/153/153.pdf

[67] http://www.cabinetoffice.gov.uk/media/cabinetoffice/corp/assets/publications/reports/intelligence/annualir0506.pdf; http://www.publications.parliament.uk/pa/cm200809/cmhansrd/cm090507/debtext/90507-0012.htm

[68] http://www.theregister.co.uk/2008/07/16/scope_network_frozen/ citing kablenet

forces in getting personnel quickly to where they are needed, for broad surveillance, for traffic management and as a general deterrent. But they are also expensive to purchase, maintain and operate. Each police force needs to make its own calculations of investment against benefit. Further investment in collecting communications data and intercept product should surely depend on the same discipline.

3. We need a view as to whether the overall UK budget for law enforcement and security is "balanced". For example, how does the Home Office £2bn figure relate to the annual cost of running the UK's main agency concerned with Serious and Organised Crime? SOCA's annual budget is just under £500m[69]. The new Police e-Crime Unit (PCeU) will receive just over £1m a year in real new money, the balance coming from the existing finances of the Metropolitan Police, plus whatever the Unit can get from industry partners. How does the demand for more law enforcement powers fit in with the statistics that show that, overall, crime in the UK is falling, not increasing?[70] In relation to fraud, a Freedom of Information Act (FOIA) request by the *Independent on Sunday* showed that there were on 788 police officers tasked with dealing with fraud, and even this is thought to be an exaggeration as many of those officers also have other duties. Some police forces, including Essex, North Yorkshire, Hertfordshire and Lancashire, have no current specialist officers.[71]

Regarding the specific costs of developing the kit for this form of surveillance, the DPI-equipment will have to be developed, and repeatedly reprogrammed, involving the expertise of highly-skilled engineers. It will have to be regularly upgraded, at least as often as the telecommunication infrastructure itself is.

The storage of the data in databases run by CSPs to support live queries is relatively complicated to do. This technology will have to be kept up to date, using some of the latest innovations and research, on par with the type of research going on in the search engine industry. The technologies and expertise for a programme of this scale are significant, and only a handful of companies could manage such a task.

Finally, the government will need a large amount of people to make the analysis decisions when presented with the data, a task that is well beyond the responsibilities of the average police officer or government official. The quantitative skills required for analysing such data are highly valued in the private sector, and thus hiring such expertise will come at an expense. Similarly the technical skills required to remotely operate DPI equipment are in premium demand in industry, and the government maintaining an expertise in-house will come at a high price.

---

[69] http://www.soca.gov.uk/assessPublications/downloads/SOCA-accounts-200708.pdf

[70] See also page 35

[71] http://www.independent.co.uk/news/business/news/fraudsters-face-uks-extremely-thin-blue-line-1689922.html

Development costs will also be high. Although there has been much research and development into DPI, it has never been attempted at this scale.

The bulk of the costs will be incurred by the CSPs. The most ignored cost comes in the form of opportunity costs as engineers will be tasked to develop this solution instead of developing their core business, i.e. new ways of enhancing the networks for advancing consumer and business interests. Engineers will certainly be needed, but there will also be a significant amount of system design on a case-by-case basis as CSPs will have to decide where to put the tap into the network, work out the space budgets for new kit, and business strategists will have to decide how to fit the DPI-kit into their plans for innovation. This could seriously hamper growth within the CSP industry.

The risks to business increase because of the increased complexity to the systems. For example, one CSP did an upgrade to all of its DSLAMS (Digital Subscriber Line Access Multiplexer) that ended up in failure. Unfortunately the firm could not roll back the upgrades, and had to send an engineer around the core parts of its network. This ended up taking three days, at great cost and inconvenience to the CSP and its customers.

To conclude, there have been a number of reports that the Government has already allocated £12bn for this policy, though there haven't been any strong confirmations regarding this amount, or the extent to which it covers all plans under the Interception Modernisation Programme. The consultation paper says that the government budgets that the range of options under consideration can cost up to £2bn, but they government appears unwilling to discuss how it came to these figures. From our consultation, however, the larger figure seems quite realistic considering how much the DPI equipment would cost, the numbers of such kits that would be required to cover the United Kingdom telecommunications sector (the large and medium sized providers at a minimum), and keeping the kit up to date.

Concluding Remarks

The United Kingdom is already a leader in communications surveillance policy. That is, the United Kingdom often has the most expansive communications surveillance regimes in the democratic world. By raising the IMP, the United Kingdom Government is again leading the debate by pushing for new collection and greater powers on a previously unseen scale. The purpose of this briefing is to ensure that the debate is informed.

When the Regulation of Investigatory Powers Act was introduced in 2000, it was one of the most advanced policies of its kind in the world. Although it contained many policy weaknesses, in the debates in and out of Parliament the intricacies of the definitions of 'communications data' and 'service provider' were more detailed than debates in most other countries. Similarly, when data retention policies were introduced from 2001 onwards, the deliberations in Parliament and across industry were of a level of detail that few other countries have seen. Even as the European Union pushed data retention through its own policy on data retention, that policy was fraught with problems because the level of understanding about the issue they were dealing with was limited, which is something that the UK Presidency seized upon.

The amount of knowledge within the UK's policy circles places the UK in a promising position as the government embarks on yet another challenging policy debate. This is not to say that the level of technological knowledge in the policy debates is ideal, however. In fact, there remain numerous weaknesses in the existing legal regimes.

Part of the problem is the very framing of the debate. This change in policy is linked with changes in telecommunications services, the complexities of communications technologies, the changes in the marketplace, and the changing expectations of governments.

The fundamental questions are thus as follows:

- Should Governments, regardless of all other considerations, have the right to access information about its citizens' communications?
- Just because a power existed in the past, such as the power to intercept post and telegraphs, because the communications infrastructure permitted it, must this power exist in the future irrespective of technological change?
- Can policy foresee the way we will use technology in the future? Will policies such as IMP change the way we use technology, and if so, is this a problem?

- Is information about communications (traffic data) less sensitive, equally sensitive, or more sensitive than the content of communications?
- Is the mere collection of information an interference with the private life of an individual or is the interference only encountered upon the accessing of that information and its use and analysis?
- Is law a sufficient safeguard against the misuse of surveillance powers? Or is a better safeguard to not build the system to begin with?
- Is it better to surveil a segment of a population, e.g. all suspects or all likely suspects, rather than the general population? Is this easier or more difficult for the industry?
- Is the 'content' of an internet communication defined by the communication protocol or is it defined by the application, or by the government?
- What are the public policy considerations in surveillance policies? e.g. costs, alternatives, regulatory implications, feasibility, etc. and should these be considered in the 'balancing' of rights?

Only when we consider these questions we can assure ourselves that we are fully considering the policy proposals.

We can only hope that attempts to address the above questions, amongst others, and the quest for policy alternatives will only continue through the debates around this policy.

Appendix 1: Issues around the Admissibility of Intercept Evidence

1. **Law of Interception.** Interception of the content of telephone calls, emails, etc is admissible in common law but excluded by statute – currently s 17 RIPA 2000. Consensual interception is admissible and so is interception material lawfully acquired outside UK jurisdiction. The general effect is to allow interception warrants but to deny their existence for court proceedings – this applies to both prosecution and defence. The detail of how this is handled appears in the CPS *Disclosure Manual*[72] – the *Manual* acknowledges many difficult areas of judgement.[73] There are also Guidelines from the Attorney General's in relation to s 18 of RIPA. [74] s 12 of RIPA empowers the Secretary of State to order communication service providers to install facilities for interception subject to certain limitations.
2. Communications / traffic data – who called whom, when and for how long - is admissible under Part I Chapter II RIPA 2000. Such evidence is often produced in conspiracy trials to demonstrate a common purpose among a number of people. Commercially available software packages to identify patterns aid this exercise and produce persuasive graphics[75]. Data traffic also includes details of which cellphones were registered to which specific base stations thus bringing the geographic locations of individuals into evidence – this is called cellsite analysis.
3. There are frequent occasions when the production of evidence based on data traffic together with other evidence before the court makes it wholly obvious that interception has taken place, though neither prosecution nor defence are allowed to refer to it. In the recent *Operation Crevice* trial (also known as the fertiliser bomb trial), which lasted over a year, although extensive use was made of conversations acquired via audio bugs, including discussions about proposed bombing of the Ministry of Sound night-

[72] http://www.cps.gov.uk/legal/section20/chapter_a.html#148

[73] http://www.cps.gov.uk/legal/section20/chapter_e.html

[74] http://www.cps.gov.uk/legal/section20/chapter_a_annex_i.html

[75] For example, *Analyst's Notebook* by I2

club and the Bluewater Shopping Centre, no reference was ever made to telephone intercepts. After the trial it was said that in excess of 100 intercept warrants had been used. [76]

4. The repeal of s17 RIPA 2000 would have the effect of *allowing* intercept material to be admitted; it would in no way *compel* it.

5. **The arguments against allowing interception evidence to be admitted.** The arguments against allowing interception evidence to be admitted are said to be[77]:

    - that knowledge of the technical means used would assist wrong-doers and make the task of law enforcement and intelligence more difficult
    - that employees of law enforcement would be placed at significant risk
    - that the process of disclosure would force law enforcement agencies to reveal more than was safe about their methods
    - that the expense to the intercepting agency of storing the material would be considerable
    - that compliance with disclosure requirements would involve the transcribing of large quantities of conversational material which in turn would be very costly
    - that it would be difficult to prove who was talking to whom
    - that innocent third parties who had had contact with an accused might find their privacy compromised

6. Nearly all of these are based on mis-conceptions either of technology or of the application of the criminal justice system.

7. **Knowledge of the existence and reach of interception** The existence of interception facilities in the UK is not a secret; the power to carry out interceptions is enshrined in statute and each year the Interception Commissioner states the number of warrants in force.[78]

8. **The Technology of Telephone Interception** There is nothing complicated or secret in the principles of how interception of landline and cellular phones take place or how to capture Internet-related (IP – Internet Protocol) traffic. For conventional, voice-based telephony two elements are required: the voice component (by placing simple circuitry across the line or by capturing digitally) and the "traffic" component - who

---

[76] http://www.telegraph.co.uk/opinion/main.jhtml?xml=/opinion/2007/06/11/do1102.xml

[77] Based ton the Report of the Interceptions Commissioner for 2005-2006, paragraph 46. http://www.official-documents.gov.uk/document/hc0607/hc03/0315/0315.pdf , the Report of the Chilcot Committee, http://www.official-documents.gov.uk/document/cm73/7324/7324.pdf and a 1999 Home Office document produced prior to RIPA and which is no longer on the Home Office website.

[78] http://www.official-documents.gov.uk/document/hc0607/hc03/0315/0315.pdf

called whom, when and for how long – which is part of the regular record of the telecommunications company for revenue collection and quality of service purposes and already admissible.

9. There are two linked elements to the technology: the handover interface between the telecommunications or communications company; and the means to record what is handed over.

10. Information about the handover interfaces for the various types of telecommunications services is published on the website of the the European Telecommunications Standards Institute (ETSI) – http://portal.etsi.org/li/Summary.asp. The actual standards are also published at http://www.gliif.org/, the Global Lawful Intercept Forum. The US equivalents, designed to work under CALEA, Communications Assistance for Law Enforcement Act, are published by the Telecommunications Industry Association (TIA) and the Alliance for Telecommunications Industry Solutions (ATIS). The ATIS website sells the current specification documents: https://www.atis.org/docstore/. Details of the application to cable-based systems can be found at http://www.cablelabs.com/specifications/archives/PKT-SP-ESP-I03-040113.pdf

11. The main features are conversion between technical protocols and the ability to guarantee and preserve the reliability of the intercepted material. The voice and the traffic components (referred to in the literature as the IRI, Intercept-Related Information) are designed to be forensically inextricably linked as a control against tampering and editing – the voice file and information about the call including the various terminating phone numbers, time and duration of call, are all held together as a single item when handed over to the Lawful Intercept authority, whoever that is.

12. Significant detail is published by vendors of law intercept equipment such as ss8 – www.ss8.com.

13. Turning now to the technology for recording telephone intercept, there is no reason why it should not be very similar to that used in call centres throughout the UK and the world – by financial institutions, government departments such as social services and the tax authorities, and mail order companies. The voice component is no longer stored on tape but as a digitised audio file on hard-disk. It is stored in a database searchable by time, date and any other fields that the user organisation deems helpful. Banks store, among other things, by account number and clerk/operator (I have seen such systems in the course of professional instructions). A lawful intercept system would, presumably store the audio files by reference to date, time, originating and receiving phone numbers, names of suspects, and warrant. Some of the products available in the open market also claim to be able, to a limited extent, to use computers to monitor the *content* of call.

14. Once data is collected digitally, the cost of storage and back-up is minimal. One would imagine that there are powerful arguments within intelligence analysis for retention in case later events give greater significance to individuals initially thought of as relatively

unimportant. Within financial services, voice data, along with everything else, is routinely held for at least seven years (Statute of Limitations requirements).

15. It would be very surprising if the UK government were using anything markedly different – current policy is to use and adapt Commercial Off the Shelf (COTS) products where-ever possible.

16. Lawful intercept also has to work for data as well as voice, including Internet-based material. Here again the websites of companies such as ss8 describe the equipment they offer and the specific types of data traffic including that for the world-wide web, email, peer-to-peer[79] networking, instant messaging, chat-room services and VOIP (voice over internet protocol which is a telephone-like service).

17. **Sensitivity of Interception Methods** The above descriptions apply to the vast majority of intercepts, which are carried out with the full co-operation of the communications service providers. Different considerations may apply where the co-operation is not available and where technicians may, for example, eavesdrop on radio, satellite and microwave transmissions or break into a cable. But this must refer to a tiny minority of instances and those are presumably concentrated on overseas activities and for intelligence purposes. As we will see shortly, there would be no legal compulsion to disclose any of this. In effect there is probably a greater argument for hoping to keep secret the technologies of audio and video probes. Here great strides have been made both in miniaturisation and also in the use of cellphone facilities as a means of transmitting the product – the earlier generation used low power radio transmitters which meant that a receiver had to be located close by; with cellphone technology the product can be received anywhere there is a phone line, mobile or fixed and there are also greater opportunities to turn probes on and off remotely at will. Audio and video probe evidence is fully admissible; it is only telecommunications intercept material which is covered by s17 RIPA.

18. **Impact on Interception Staff** If one thinks about what is involved in accepting a lawful intercept from a co-operating communications service provider, this has to be one of the least dangerous activities carried out by an agency. The operator stays in his office and uses a keyboard, a telephone, a screen, and a loudspeaker. The installer of a voice probe, the product of which is admissible, must covertly visit hostile territory; the agent handler, physical surveillance operator and under-cover personnel must all go out into the "field".

19. **Disclosure Regime** The applicable law is Criminal Procedures and Investigations Act, 1996 (as amended, particularly by the Criminal Justice Act 2003[80]). Practical detail appears conveniently in the CPS *Disclosure Manual.*

---

[79] As used in file-sharing services

[80] Part 5

20. The principles are that any material gathered in the course of an investigation but which is not specifically adduced in evidence must be recorded and retained; it must be revealed to the case prosecutor who applies a "disclosure test", which means "providing the defence with copies of, or access to, any material which might reasonably be considered capable of undermining the case for the prosecution against the accused, or of assisting the case for the accused, and which has not previously been disclosed." At the "revelation" stage, a police officer can mark material as "sensitive unused" ; the test for this being that disclosure would give rise to "a real risk of serious prejudice to an important public interest"; reasons must be given. [81] In due course this may give rise to applications for Public Interest Immunity certificate. Throughout there is a continuing duty to disclose.[82]

21. But there is also an obligation on the Defence to provide a defence case statement, once initial prosecution disclosure has taken place. The CPS *Disclosure Manual* provides convenient details of what is required of defence case statement at Chapter 15. Failure to provide such a statement, which has to occur within specified time limits, can result adverse inferences being drawn at trial.[83] These can include differences between what is set out in a defence case statement and what is relied on in trial.

22. The detail of how this is currently handled in relation to intercept material appears in the CPS *Disclosure Manual* in Chapter 27 and in relation to unused forensic science material (which may be relevant to specific methodologies of interception) at Chapter 23.

23. The position of experts instructed by the defence also needs to be considered. In general terms: a defence expert, whether giving evidence of the results of a technical investigation or (if allowed by the judge) of opinion, has an over-riding duty to the court.[84] Advice given prior to evidence is legally privileged. Investigations carried out by the defence expert have in broad terms to comply with the defence case statement. The fact that a defence expert has been instructed must be disclosed even if the evidence is later not relied on[85]. Specific disclosure would only follow a detailed and consistent defence case statement. A defence expert receives information relating to a case solely for that purpose and cannot refer to it elsewhere unless it is also mentioned in open court; breach can result in contempt of court proceedings. . The prosecution has the ability in pre-trial hearings to question the quality and *bona fides* of a defence expert and there are opportunities to seek undertakings and court orders in respect of

---

[81] *CPS Disclosure Manual* Chapter 8

[82] s 7A CPIA

[83] s 11 CPIA 1996, s 39 CJA 2003.

[84] Criminal Procedure Rules, Part 33. http://www.justice.gov.uk/criminal/procrules_fin/contents/rules/part_33.htm

[85] s 35 Criminal Justice Act 2003, amending s 6, CPIA, 1996

defence experts. For example, this is already done in terms of sensitive computer hard-disk evidence and where the expert may need to visit covert law enforcement and other premises.

24. **How disclosure of intercept material would work in practice** Whereas a few years ago voice intercept material was recorded to reel-based tape recorders current methods record to digital audio file saved to hard-disk, each audio file being linked to a database.[86] This should significantly ease the practical problems of disclosure. The defence would receive CDs or DVDs containing the audio files plus the accompanying data (which number called which, when and for how long for conventional telephone intercepts, for example). Only material to be used in evidence would be initially transcribed by the prosecution; otherwise the defence would listen to the audio and, should they wish to adduce additional material, they would transcribe it. If there were disputes about what was being said, most can be resolved pre-trial between counsel and experts. Under current Criminal Procedure Rules a trial judge can order experts to have meetings to reduce the scope of a dispute. [87] This approach is what currently happens in relation to evidence from computer hard-disks where the whole of the hard-disk is disclosed in electronic form and only very small portions ever printed out. It is also what has been done in the case of audio probe evidence (which is currently admissible).

25. If we now consider the impact in terms of the objections usually raised in relation to the abolition of s 17 RIPA:

    - costs of routine disclosure would not be high – transcription of everything is not required; the material is held and used in digital format and data storage and copying costs are very low; much higher costs are routinely incurred in relation to computer hard-disk evidence
    - under normal circumstances the defence could test for tampering by reference to the records created by the lawful intercept hand-over equipment, the separate routine records of traffic date produced by communications service providers (which are currently admissible and regularly produced) and the length of time of each audio file. All ought to match. In addition they could instruct a specialist audio expert to look for anomalies in the digital audio file
    - in order to obtain further detailed knowledge of specific technologies, the defence would need to refer to them in a defence case statement and be prepared to justify such reference later if nothing adverse to the prosecution were found; the penalty for a defence fishing expedition would be that adverse inferences might be drawn against the defendant.

---

[86] See para 13 above

[87] Part 33.5 http://www.justice.gov.uk/criminal/procrules_fin/contents/rules/part_33.htm

- it is difficult to envisage a successful defence disclosure request which might refer to such potentially sensitive information as the overall capacity to intercept or the extent to which automated monitoring of intercept material is possible (for example by listening for keywords or looking for indications of voice-stress) as these would usually not be relevant to any specific case. It should also be borne in mind that what a terrorist planner surely really wants to know is are those circumstances in which the authorities find it most difficult to intercept, the principle that it is possible and occurs is already well-known
- it would still be open to the prosecution to raise PII issues against the usual tests as with other types of sensitive evidence such as covert human intelligence sources.
- the normal use of intercept evidence would be to show planning, intent, or "bad character"[88]. The usual stances of the defence will include: that the prosecution have misidentified the speakers; that the selected passages are being misinterpreted as to significance and meaning; that by also referring to other conversations in the unused material, a different light is shed on the motivations of an accused. But all these are within the normal scope of court activity and in any event applies to audio probe and computer hard-disk[89] material that are currently admissible.
- the rights of third parties who had innocent connections with an accused and who conversations with them might have been intercepted will be preserved in the same way as innocent people who have email contact with suspects and whose emails are found on hard-disk. The innocent conversations will only be seen/heard by lawyers and experts and will not be used in open court. Abuse of such data would be a contempt of court.

[88] Possible, subject to certain judicial safeguards, under ss 98 ff Criminal Justice Act 2003.

[89] A frequent issue with personal computers used by several people is "whose fingers on the keyboard at the relevant time?

Appendix 2: The Privacy Issues

Much of the discussion in this paper focussed on the effects of the policy on the technology, the industry, and government agencies. We must also give consideration to the real implications for individuals, end users, consumers, and citizens.

Although there is a case for the new powers, a thorough analysis of all citizens' communication traffic data would radically transform British society. Private meetings would be a thing of the past. This would be akin to having to notify the government of all the people you met with last night, in order to give them the opportunity to choose whether they want to retrospectively read any conversation transcripts that may be available. This has profound implications for the ability to associate free from surveillance.

Political campaigning and political organising would be radically transformed. Political actors would be under constant scrutiny, regardless of whether their communications data is actually being physically read by an individual. For instance, CSPs would be called on to hold all the detailed transaction information of every Member of Parliament and every journalist: their phone calls (to lobbyists, colleagues, constituents and sources), locations, website viewings, social networking, and chats. It is a map of everyone's private life, but also his or her professional and social life too.

Since our telecommunication infrastructure is also used as part of our critical infrastructure, such operations will also be under constant surveillance. The approximate location over every person carrying a mobile device, including police officers, military officers, ministers, civil servant or business will be on record, and accessible in real-time. This information would be invaluable to foreign intelligence, to extract information or gather blackmail material, as recent cases in of unlawful interception in Greece and Italy illustrate.

Importantly, this is not just the personal information of the individuals whose account records are being accessed. It is also the personal information of those with whom the 'suspect' individuals are communicating. As more on-line services create shared public spaces, putting a single individual under surveillance will inevitably lead to the collection of third-party communication data. For example gathering the traffic data relating to a suspects on-line presence, will also gather whether their list of contacts are on-line or off-line. Observing a location-based service is likely to reveal the location of a target's friends as well.

The Government's response to many of these concerns is merely to repeat that the power they are seeking is not the content of communications but just the information about the communications. But it is important to note that this is as least as privacy intrusive as content interception. This is not about the atoms of data, but rather the data will accessed and analysed and brought together from across channels to create a comprehensive profile of an individual's interests, intentions, associates, usual locations, and the nature of those interactions. When these processes are applied to criminal organisations they might be effective, but they also have the potential to uncover perfectly legal associations that require a level of confidentiality. Any assessment of 'proportionality' on a specific atom of data will miss that the whole picture of an individual's private and professional life can and will be seen, judged, and profiled.

In some ways communication data might even be seen as more intrusive than content since its analysis reveals attributes that are unknown to the targets. The frequency and times of communications reveal the strength and type of people's relations. The number of people two parties know in common is an indication of the social cohesion of their groups. The co-location of mobile devices, at day or night is an indicator of friendship or intimate relations. In all of those cases the subjects of surveillance are not aware that they leak such information, in contrast to when they explicitly do so in the content of their communications.

Furthermore the paradigm of seeing communications data in the context of the plain old telephone system (POTS) underestimates the reach of the inferences that can be drawn from analysis such information. The items under scrutiny include simply a list of called numbers, the time and duration of the calls. A much more appropriate parallel would be imagining the government having a deaf security agent following every single person everywhere they go. The agent cannot hear the content of any interactions, but can otherwise observe every minute detail of someone's life: the time they wake up, how they drive to work, who they talk to and for how long, and how their business is doing, their health, the people they meet in the street, their social activities, their political affiliations, the papers and specific articles they read, and their reaction to those, the their shopping basket, and whether they eat healthily, how well their marriage is going, the extra-marital affairs, their dates and intimate relations. Since most of these interactions are today mediated at some level by telecommunications services, or are facilitated by mobile devices, all of this information will now reside with our internet service providers, ready and waiting for government access.

A Chilling Effect?

As the general public becomes aware of the practice of collecting and collating all this personal information, the risk is that it will generate a chilling effect on the individual's right to free expression, association and might dissuade people from participating in communications transactions. Already, following from the media coverage of the Government 'wanting to get access to social networking profiles' there has been a rising

concern about what people do or say on social networking sites. As we try to build 'Digital Britain' we may in fact be creating a barrier to people accessing online services and applications out of fear of surveillance.

This chilling effect could, in turn, have serious ramifications for industry. If developments like 'cloud computing' and increasing virtual communications and modes of work are placed under similar scrutiny then the policy of modernising policing powers could restrict innovation, or drive infrastructure out of the UK. Every time an individual shares a document with a colleague, this process generates communications traffic data. Every online video conference or sharing of knowledge through discussion boards across organisations will generate communications traffic data over public networks. This will result in a level of surveillance never seen before, with ever weakening safeguards.