Lines on the LSE IMP report

Lines to take to address the London School of Economics' report

TECHNICAL/CSP RELATED QUESTIONS

- 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 a CSP to deploy) or on potential utility in an investigation (which would require the CSP to make judgements wholly outside their regular experience)?

- 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?

- 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?

Lines to take:

- This is a complex and extremely sensitive subject, with a fine balance to be made between protecting public safety and civil liberties. That is why the previous Home Secretary announced that the public consultation 'Protecting the Public in a Changing Communications Environment' would take place.

- No decision on a proposed solution has been made yet, and won't until the results of the consultation are known.

- Legislation will be required to maintain ability to collect communications data in the future, but a decision on new legislation and what it will include will not be made until later in the year.

SAFEGUARDS

Is the Interception Commissioner is a plausible safeguard?

There must be as there now, stringent safeguards controlling how communications can be obtained (and by whom). Independent oversight of these safeguards will be absolutely vital and central to any changes; this independent oversight is provided by the Interception of Communications Commissioner.

How many inspectors are there, what skills and experience do they possess?

The Commissioner is supported by a Chief Inspector and five Inspectors who are all highly trained in the acquisition and disclosure processes and the extent to which communications data may assist public authorities in carrying out their functions. All of the inspectors have a background in conducting criminal investigations.

Are there enough to cope with the average of 1422 communications authorisations that occurred every day during 2007 (including week-ends and bank holidays)?

The Commissioner considers that the size of the Inspectorate is sufficient to enable him to carry out his oversight responsibilities effectively.

Last year over half a million requests were made by public authorities for communications data but it is estimated that about 80% of them would be for subscriber information only. It would need an army of inspectors to look at all of these requests and this is neither necessary nor proportionate. It would also be a huge waste of public money.

All the police forces, law enforcement agencies and intelligence agencies have now been inspected at least twice and generally the outcomes of these inspections have been satisfactory.

Under the Code of Practice the Commissioner has the power to direct a public authority to provide information to an individual who has been adversely affected by any wilful or reckless failure to exercise its powers under the Act. So far it has not been necessary for the Commissioner to exercise this function but there is no room for complacency and each police force and law enforcement agency understands that it must strive to achieve the highest possible standards.

ANALYSIS

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

Yes. Distinguishing between content and communications data is still feasible and can be assessed against the definition of communications data in the Regulation of Investigatory Powers Act 2000 (RIPA).

For some communications services it is easy to differentiate between the communications traffic data, the envelope, and the content.

For other new or proprietary services the distinction can be more complex with layers of envelope, but those are addressing envelopes not content.

How do we deal with the inadmissibility of Interception Material?

Any piece of information relating to a communication can be assessed against the definition of communications data in the Regulation of Investigatory Powers Act 2000 (RIPA), the subject of a separate consultation.

Communications data will continue to be available as evidence regardless of the outcome of the current review of the use of intercept product (which is not being covered by this programme or this consultation).

Who grants interception warrants and authorises release of communications data?

The Secretary of State grants interception warrants while applications to acquire communications data under Chapter 2 of RIPA are carefully considered by a senior “designated person” within each public authority who holds an office, rank or position approved by Parliament. The designated person is independent of the investigation and will only grant the authorisation or give the notice if the tests of necessity, proportionality and legitimate aim are satisfied.

Independent oversight is provided by the Interception of Communications Commissioner, an individual who must have held high judicial office. This oversight includes regular inspections of all relevant public authorities, and others involved in the process of considering or giving effect to warrants to ensure that the powers are being exercised in full compliance with RIPA.

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

Yes it is feasible – but only in relation to ongoing investigations and not to reactive investigations following a crime. Historic communications data provides valuable intelligence and evidence of criminal conspiracy and associations, and evidence of victims' experience.

The collection of communications data enables the targeted interception of communications by providing information on the communication event that is to be targeted following an authorised warrant.

The government has never said that we are going to track and filter communications data in respect of everybody. 100% coverage would not only be impossible to achieve, but the costs involved in attempting such coverage would far outweigh any benefits there might be.

We only track those communications that are relevant to the protection of the public when investigating serious crimes such as child sex abuse, murder and terrorist activities and will continue to do so.

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

The Interception Modernisation Programme is currently investigating the many options and potential methods to enable the collection and storage of communications data by CSPs. Options are based on the federated approach as set out by the consultation and will be guided by consultation responses. IMP is considering how DPI technologies might support the lawful acquisition of communications data.

However, it is the long established policy of successive governments not to comment on matters relating to technologies that may be used to carry out lawful interception of communications or communications data acquisition. Lord West has made clear deep packet inspection is such a technology.

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?

We need separate UK legislation to cover the retention of "3rd party service data" to ensure that this category of data continues to be available for acquisition by public authorities under RIPA. This legislation will make explicit the type and quantity of communications data to be retained and matched by CSPs.

The Interception Modernisation Programme is currently investigating the potential methods needed to tell computers what to retain and will be guided by consultation responses.

Will GCHQ have access to the black boxes and if so, with what safeguards to ensure against abuse or malicious attacks from other parties?

IMP is still considering options for CSP communications data processing solutions and will be guided by consultation processes.

It is the long established policy of successive governments not to comment on matters relating to technologies that may be used to carry out lawful interception of communications or communications data acquisition. Lord West has made clear deep packet inspection is such a technology.

Access to Communications Data is restricted to a few Relevant Public Authorities as set out under RIPA, of which GCHQ is one.

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

Without the ability to intercept and obtain retained CD, the effectiveness of law enforcement and intelligence agencies would be severely hampered.

The existing capabilities to intercept communications and obtain CD are essential tools in countering terrorism and serious and organised crime. They also make a vital contribution to public safety, proactive and reactive policing and the prevention of imminent threats to life.

Other techniques may be more intrusive and expensive and in some cases would not be capable of providing the information required.

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"?

Our ability to use communications data is essential to counter terrorism, fight crime and protect the public. Without increasing powers to access regular communications data, our ability to do this will diminish.

As Bill Hughes, Director General of the Serious Organised Crime Agency said recently:

> "Using communications data and intercept intelligence are key factors in over 95% of the most significant investigations directed at the serious organised crime groups assessed as causing the most harm to the UK."

We recognise that people might interpret this as needing to make sacrifices, which is why we are determined that any solution proposed by the IMP will follow a solid legal framework that protects civil liberties.