Media enquiries contact 0207 340 6030 / 07505 448925
press@bigbrotherwatch.org.uk

Communications Capabilities Development Programme briefing and summary of key issues

Key Questions:

- Will there be a white list of people who won't have their activity logged? (For MPs – Wilson Doctrine, diplomats etc)
- Breaching the Data Protection Act is currently not eligible for a custodial sentence; will this change to deter staff selling data held by service providers?
- What is the estimated cost to the taxpayer?
- The Oxford Internet Institute, LSE and Cambridge Computer Lab have all seriously questioned the feasibility of this – given the past experience of Government IT schemes how is this not going to be another feeding frenzy for the big IT contractors?
- Can the Home Secretary offer any example of this being done in another country?

Key Issues:

- Breaching the Data Protection Act can only be punished with a fine, not a custodial sentence so there remains a serious risk any stored data could be lost or mis-used.
- Will there be a 'white list' of people who are not monitored, for example MPs or foreign diplomats.
- Why has this not been put in place before the Olympics if it is so crucial?
- Will higher level of encryption and the use of Tor/Proxies render the programme far less useful than is being claimed?
- Will threats be driven underground or into 'dark nets', making them harder to detect?
- Why does no other democratic state have this kind of monitoring
- The use of RIPA to obtain data does not require a judicial warrant – except by local authorities. Will RIPA be amended to restrict use of communications data to police and security services?
- What will the cost be for Government and for the economy, particularly in terms of investment in high-speed internet access and data-driven companies moving abroad?
- Once monitoring capability is installed, will proposals for controlling what web content can be seen be the next step?

The Use of RIPA By local authorities:

Local authorities cover a tiny fraction of the comms data requests and as such this concession is nothing short of deliberate misdirection. Since 2005, there have been more than 2.7 million requests by police and other public bodies for the communications data belonging to private individuals. Little more than 3,000 requests came from local authorities.

The Coalition Agreement states:

- "We will implement a full programme of measures to reverse the substantial erosion of civil liberties and roll back state intrusion."
- "We will end the storage of internet and email records without good reason."

The 7/7 Inquest stated:
"Post 7/7 enquiries revealed that between 22nd February and 15th June 2005 there were forty one telephone contacts between mobile phones attributed to Tanweer, Khan, and Lindsay and hydroponics outlets. It is unlikely these could have been detected by surveillance given the large number of untraceable "operational" phones used by the bombers and only attributed to them once their identities and details were known."

'We need to take very great care not to fall into a way of life in which freedom's back is broken by the relentless pressure of a security state.'
Sir Ken McDonald, former Director of Public Prosecutions, 2008:

The Prime Minister, David Cameron said before the election:

"Faced with any problem, any crisis – given any excuse – Labour grasp for more information, pulling more and more people into the clutches of state data capture… And the Government doesn't want to stop with the basic information. They want the most complex, important, personal information there is… Scare tactics to herd more disempowered citizens into the clutches of officialdom, as people surrender more and more information about their lives, giving the state more and more power over their lives. If we want to stop the state controlling us, we must confront this surveillance state."[1]

The Conservative Policy Document, 'Reversing the rise of the Surveillance state', 2009.

Fewer personal details, accurately recorded and held only by specific authorities - on a need-to know basis only, and for limited periods of time.

Immediately submitting the Home Office's plans for the retention of - and access to - communications data to the Information Commissioner for pre-legislative scrutiny.

[1] http://news.bbc.co.uk/1/hi/uk_politics/8119047.stm

Further analysis:

- If this is such an essential capability, why did the Government not ensure it was in place before the Olympics and diamond Jubilee celebrations?
- Why has no statement been made to Parliament on this issue?
- Ministerial statements in the media have assured the public no new capability is being proposed – yet there is currently no ability for real-time monitoring – which is correct?
- Is this about preventing a terrorist attack, or assisting investigations afterwards?
- Can the Home Office point to any other democratic country that has a similar system in place?
- The existing data retention directive is currently being challenged in the European Court of Justice – to what extent is this policy compatible with Article 8 of the European Convention of Human Rights?
- How is this policy compatible with the Coalition Agreement pledge to 'end the storage of email and internet records without good reason'
- Is there a danger that whistle-blowers will be deterred if they can be identified by data collected?

On the details:

- What risk is there that this surveillance will drive dangerous individuals underground?
    - (One by-product of the Internet Watch Foundation's list of websites (which are blocked by most UK ISPs) has been to drive child abusers into non-web based communications.)
- Can the Home Office confirm what data will be required to be retained?
    - Will this include geo-location data?
- If an email or other web communication is encrypted, is it even possible to read the 'header' data without also exposing content?
- How will virtual private networks – used by companies to enable staff to work from home securely – be affected by this policy?
- How will this impact on companies who do not have a physical presence in the UK (or indeed EU)
- Will this require deep packet inspection of internet traffic, and if so how is this compatible with existing legal precedent that this is unlawful?
- In the 7/7 inquest the obstacle of unregistered 'operational' phones was raised as a key obstacle to the value of increased surveillance – how will this proposal address that problem?
- The Home Secretary highlighted Ian Huntley as one example of how this proposal could help, yet the official enquiry recognised more data was not the solution, it was information sharing. (quote below)
- What assessment has been made of the risk that real-time monitoring and increased data retention could introduce new security vulnerabilities to the internet, offering both criminals and foreign governments opportunities to gather data that do not currently exist.

On the Regulation of Investigatory Powers Act:

- Serious concerns exist about who will access this data – will the Home Secretary bring forward in this Bill a proposal to restrict access under RIPA to communications data to the police and security services?
- Last year Google rejected 37% of the requests made to it for service user data by UK authorities – how will the real-time access ensure that there is any check or balance on requests for data?
- Will the Home Secretary commit to publishing the number of communications data requests made under the existing system, by whom and for what purpose, as part of the Bill's consultation?
- How will safeguards against the real-time access work if there is no judicial authorisation?

On the economic impact:

- How significant a cost on businesses
- Under the current system data requests are paid for by the requesting body -
- Has any consideration been given to whether CCDP will be a deterrent to companies investing in new infrastructure (fibre optic broadband, 4G etc.) and what liaison has the Home Office undertaken to evaluate this?
- What assessment has been made that companies will use this retention as a Trojan horse to collect even more user data for commercial purposes

On being different to Labour's plans:

- In 2009 the Home Office held a consultation on the possibility of requiring internet service providers (ISPs) and telecommunications companies, who are qualified as 'Communications Service Providers' under UK law
    - This proposal appears to directly replicate this policy, further contradicting the assertion this is a different plan
- Labour's proposal for one database and the CCDP plans for many service-level databases are only semantically different. Surely the question is whether the same amount of data is being collected as would have been the case under Labour's plans?
- Responding to Big Brother Watch's Freedom of Information requests, the Home Office has denied that a draft Communications Data Bill (2008) was written, saying the Government decided not to bring forward such a draft Bill.
- However, the Cabinet Office responded to the same request saying:

"The Office of the Parliamentary Counsel) does hold information falling within the terms of your request. The information is however being withheld as falling within the exemptions in s35 (1) of the Freedom of Information Act 2000 (formulation or development of government policy) and s42 (Legal professional privilege."

Compare and contrast the Labour Home Secretary's arguments with those of the current Home Secretary.

Jacqui Smith: "Communications data is used as important evidence in 95% of serious crime cases and in almost all security service operations since 2004."

Theresa May: "Such data has been used in every security service terrorism investigation and 95 per cent of serious organised crime investigations over the last ten years."

On Labour's plans:[2]

Shadow home secretary Dominic Grieve, said the government's record on protecting data was "appalling" adding: "Putting all this data into the hands of the government will threaten our security, not make it better."

Liberal Democrats home affairs spokesman Chris Huhne said the database would be "an Orwellian step too far".

[2] http://news.bbc.co.uk/1/hi/uk_politics/7507627.stm

The Use of Communications Data:

The Regulation of Investigatory Powers Act 2000 (RIPA) came into effect in September 2000. It establishes a regulatory framework for the acquisition of communications data by setting up an authorisation procedure. Communications data are defined in Section 21(4) of RIPA and include information held by any postal service or telecommunications service or system. RIPA seeks to ensure that public authorities only acquire communications data where it is necessary for a specific, legally prescribed purpose, and that the acquisition is carried out in such a way that the risk of infringing the rights of individuals is kept to an absolute minimum.

Acquisition of Communications Data is not just limited to the security services.

"Cheshire West and Chester Council will on occasion need to acquire communications data in order to carry out its enforcement functions effectively. Examples of enforcement activities which may require the acquisition of communications data include, in particular, trading standards investigations relating to doorstep crime, counterfeiting and other fraudulent trading activity. **A local authority may only acquire communications data for the purpose of the prevention or detection of crime or the prevention of disorder."**[3]

Communications Data that can be acquired[4]

The types of information that can be accessed from a Communications Service Provider (CSP) fall into 2 categories.

Subscriber Information (RIPA S 21(4)(c)) - Information about communications services users

- Name of the customer who is the subscriber for a telephone number, an e-mail account, PO Box number, a Post Paid mailing stamp, or is entitled to post to a web space;
- Account information such as address for billing, delivery or installation;
- Subscriber account information such as bill paying arrangements, including details of payments and bank or credit/ debit card details;
- Information about the provision of forwarding and redirection services;
- Information about connection, disconnection and reconnection of services the customer subscribes to, including conference calling, call messaging, call waiting and call barring telecommunications services;
- Information provided by the subscriber to the CSP such as demographic information or sign up data (other than passwords) such as contact telephone numbers;

- Information about telephones or other devices provided by the CSP to the subscriber and associated codes, including Personal Unlocking Keys for mobile phones & serial numbers;

[3] Cheshire West and Chester Council: Acquisition & Disclosure of Communications Data

[4] http://www.rctcbc.gov.uk/en/relateddocuments/publications/tradingstandards/ripacommunicationsdatapolicydec2010.pdf

Service Use Data (RIPA S 22(4)(b) – Information about the use of communications services

- Periods during which the customer used the service;
- Activity including itemised records of telephone numbers called, Internet connections, dates and times of calls, duration of calls, text messages sent and quantities of data uploaded or downloaded;
- Information about use made of forwarding and redirection services;
- Information about the use made of conference calling, call messaging, call waiting and call barring telecommunications services;
- Information about the selection of preferential numbers or discount calls;
- Records of postal items, such as records of registered, recorded or special delivery postal items and records of parcel consignment, delivery and collection;
- Top-up details for pre-pay mobile phones including credit/ debit card, voucher/ e-top up details;

There are two powers granted by S22 RIPA in respect of the acquisition of Communications Data from telecommunications and postal companies ("Communications Service Providers").

In order to compel a Communications Service Provider to obtain and disclose, or just disclose communications data in their possession, a notice under S22 (4) RIPA must be issued. The sole grounds to permit the issuing of a S22 notice by a Local Authority is for the purposes of "preventing or detecting crime or of preventing disorder". The issuing of such a notice is likely to be the main power utilised by us, in those circumstances where the Council SPOC liaises directly with the Communications Service Provider.

In addition S22 (3) provides that a Designated Person can authorise another person within the same relevant public authority to engage in specific conduct to collect the data. This allows the local authority to collect the communications data themselves, e.g. if a Communications Service Provider is technically unable to collect the data, an authorisation under this section would permit the local authority to collect the communications data themselves.

Commonly this will occur if there is an agreement in place between a public authority and a CSP relating to appropriate mechanisms for disclosure of communications data directly to the authority. The authorisation describes the conduct that is authorised and describes the communications data to be acquired by that conduct. Where a SPOC has been authorised to obtain subscriber details but then concludes that the data is held by a CSP from whom it cannot be acquired directly, rather than obtaining a notice, the SPOC can provide the CSP with details of this authorisation in order to seek disclosure of the required data.

Examples of Communications Data Use

The following examples have been obtained by Big Brother Watch under the Freedom of Information Act.

Organisation	Year	Nature of Offence
Child Support Agency	2011-2012	Conspiracy to defraud, Fraud by Misrepresentation, Providing false information
Northumberland County Council	2009-2010	Tarmac Surfacing
Stockton Borough Council	2009-2010	Movement of Pigs
		Fraudulent Escort Agency
London Borough of Merton	2009-2010	Fraud, breach of trade descriptions Act and conspiracy
	2008-2009	Unfair trading - communications data request
Kent County Council	2008-2009	Cold calling - Cancellation Notices/Fraud/Consumer Protection from Unfair Trading Regulations

Since RIPA came into force in 2000, there have been:

- more than 20,000 warrants for the interception of phone calls, emails, and Internet use;
- at least 2.7 million requests for communications data, including phone bills and location data;
- more than 4,000 authorisations for intrusive surveillance, eg, planting bugs in someone's house or car;
- at least 30,000 authorisations for directed surveillance, eg, following someone's movements in public, or watching their house.

Since 2005, there have been more than 2.7 million requests by police and other public bodies for the communications data belonging to private individuals, including more than 3,000 requests by local authorities

Challenging the myths around communications Data:

Writing in the Sun, the Home Secretary said:

"Data like this has already helped lock away murderer Ian Huntley."

Did it really?

The Ian Huntley official enquiry said:
"It emerged that Huntley had been known to the authorities over a period of years, coming into contact with the police and/or social services in relation to 11 separate incidents involving allegations of criminal offences, between1995 and 1999. Nine of these were sexual offences. This was not discovered in the vetting check carried out by Cambridgeshire Constabulary when he was appointed caretaker of Soham Village College late in 2001."

There are also serious questions about feasibility that were raised in the 7/7 Inquest:

The Coroner's report discusses the issues involved with large amounts of data and surveillance:

"However, one must never lose sight of the fact that the material confronting the Security Service at the time would have comprised literally thousands of strands of intelligence of varying degrees of quality, in relation to thousands of possible contacts and hundreds of possible targets. The desk officers must usually work at speed and in very difficult conditions. We do not know the precise details, but we know enough properly to infer that the sheer scale and number of the threats facing the UK was immense. If one plot is discovered to involve an imminent threat to life resources must be diverted to meet it at the expense of other investigations."

"Post 7/7 enquiries revealed that between 22nd February and 15th June 2005 there were forty one telephone contacts between mobile phones attributed to Tanweer, Khan, and Lindsay and hydroponics outlets. It is unlikely these could have been detected by surveillance given the large number of untraceable "operational" phones used by the bombers and only attributed to them once their identities and details were known."

"There was some evidence on the question of the quality of the software supplied to the Security Service. G gave evidence that "it can be very difficult" to "dig into" the files and computer systems at the Security Service to try to find out if a particular person has previously come to their attention. Witness G was pressed on the ease with which the Security Service could, today, retrieve all references to someone with the surname Khan. He explained the difficulties given the large number of people bearing the name Khan. Inputting even the name Siddique Khan, for example, may not produce helpful results."

Parliamentary Questions about the Communications Capabilities Development Programme:

15 Nov 2010

Simon Wright: To ask the Secretary of State for the Home Department if she will bring forward proposals to put her Department's Interception Modernisation Programme on a statutory footing; and if she will make a statement. [20464]
Nick Herbert: As was made clear in the strategic defence and security review, the Government will continue to build on an existing programme of work to preserve the ability of the law enforcement, security and intelligence agencies to obtain communications data and to intercept communications within the appropriate legal framework. We will legislate to ensure this is compatible with the Government's approach to civil liberties and use of communications capabilities. Details of this legislation will be announced in Parliament in due course.

22 May 2012

Mr Carswell: To ask the Secretary of State for the Home Department whether she plans to include non-UK based internet service providers in the Communications Capabilities Development Programme. [107071]

James Brokenshire: The Queen announced on 9 May 2012 the Government's intention to bring forward measures to maintain the ability of the law enforcement and intelligence agencies to access vital communications data under strict safeguards subject to scrutiny of draft clauses. Further details of this legislation will be presented to Parliament in due course.

24 April 2012

Mr Raab: To ask the Chancellor of the Exchequer what estimate he has made of the sum required to fund the Communications Capabilities Development Programme; and whether such funds have been set aside for this purpose. [104997]

Danny Alexander *[holding answer 23 April 2012]:* The Home Office are responsible for costing their programmes, including the Communications Capabilities Development programme (CCD), which has been in place since 2011.
Home Office expenditure limits were set out at the time of the 2010 spending review, details of which are available here:
http://www.hm-treasury.gov.uk/spend_index.htm
The costs of the Communications Capabilities Development programme will be announced by the Home Office alongside details of the proposals in due course.

26 Apr 2012:

Mr Raab: To ask the Secretary of State for the Home Department what assessment she has made of the technical viability of the Communications Capabilities Development Programme. [104305]

James Brokenshire *[holding answer 23 April 2012]:*The technical capabilities required for the Communications Capabilities Development programme have been selected

on the basis of proven technology. Technical viability is kept under review through periodic external assurance reviews and by consulting with industry, suppliers and other Government Departments.

Mr Raab: To ask the Secretary of State for the Home Department what formal advice she has received from the Information Commissioner on the Communications Capabilities Development Programme since October 2010. [104306]

James Brokenshire *[holding answer 23 April 2012]:* Home Office officials have consulted the Information Commissioner on the Communications Capabilities Development programme and continue to work with his team on the privacy impact assessment which will accompany any proposals.
Mr Raab: To ask the Secretary of State for the Home Department which *(a)* Government departments, *(b)* external experts and *(c)* private companies have been consulted on the Communications Capabilities Development Programme since May 2010. [104307]

James Brokenshire *[holding answer 23 April 2012]:* The Home Office has engaged with other Government Departments, the National Security Council, external experts and operational stakeholders. There is ongoing engagement with relevant industry representatives.

17 May 2012:

Mr Carswell: To ask the Secretary of State for the Home Department whether she has made an assessment of the possible effect on competition in the internet service provider market of the Communications Capabilities Development Programme. [107073]

James Brokenshire: The draft Communications Bill and related documents, including an impact assessment, will be presented to Parliament in due course.

11 June 2012

Mr Carswell: To ask the Secretary of State for the Home Department whether a notification under the Technical Standards Directive will be required prior to the implementation of the Communications Capabilities Development Programme; and if she will place in the Library a copy of any such notification. [107072]

James Brokenshire: We will consider whether a notification under the technical standards directive is required and, if so, a copy will be placed in the House Library.

Parliamentary Questions about Labour's Intercept Modernisation Plans:

Francis Maude Written Question January 2009
To ask the Secretary of State for the Home Department what the estimated (a) set-up and (b) running costs of the interception modernisation programme are. [250530]

Mr. Coaker: *The Interception Modernisation Programme (IMP) will require a substantial level of investment which will need to tie in with the Government's three year CSR periods. The scale of overall economic investment is very difficult to calculate because of the complexity of the programme and wide ranging implementation solutions currently being considered.*
Given the commercial and national security sensitivities, the precise costs of the programme cannot be disclosed. Further detail on budgetary estimates for the IMP will however become available once the public consultation process (announced by the Home Secretary on 15 October 2008) commences."

19th November 2008
Eric. Pickles: To ask the Secretary of State for the Home Department what estimate she has made of the *(a)* set-up and *(b)* annual running costs of the Interception Modernisation Programme database. [236501]

Mr. Coaker: The objective of the Interception Modernisation Programme (IMP) is to maintain the UK's Lawful Intercept and Communications Data capabilities in the changing communications environment. It is a cross-government programme, led by the Home Office, to ensure that our capability to lawfully intercept and exploit data when fighting crime and terrorism is not lost. It was established in response to the Prime Minister's National Security remit in 2006.

As part of the Government's Comprehensive Spending Review (CSR 07) a central bid was made to HM Treasury on behalf of the security and intelligence agencies. Funding for IMP was included in this bid.

The IMP will require a substantial level of investment which will need to tie in with the Government's three-year CSR periods. The scale of overall economic investment is very difficult to calculate because of the complexity of the project and wide ranging implementation solutions currently being considered.

Given the commercial and national security sensitivities, the precise costs of the programme cannot be disclosed. Further detail on budgetary estimates for the IMP will however become available once the public consultation process (announced by the Home Secretary on 15 October) commences in the new year.

23rd October 2008
Chris Huhne: To ask the Secretary of State for the Home Department what estimate she has made of the cost of the interception modernisation programme. [228993]

Jacqui Smith: The objective of the Interception Modernisation Programme (IMP) is to maintain the UK's lawful intercept and communications data capabilities in the changing communications environment. It is a cross-government programme, led by the Home Office, to ensure that our capability to lawfully intercept and exploit data when fighting crime and terrorism is not lost. It was established in response to the Prime Minister's National Security remit in 2006.

Given the commercial and national security sensitivities, the precise costs of the programme cannot be disclosed. Further detail on budgetary estimates for the IMP will however become available once the public consultation process, which I announced on 15 October, commences in the new year.

Communications Capability Development Programme (CCDP): some key technical questions: practicality, value for money

This section is reproduced by kind permission of Peter Sommer.
www.pmsommer.com
www.fipr.org
www.privacyinternational.org
http://www.lse.ac.uk/collections/informationSystems/research/policyEngagement/IMP_Briefing.pdf

The detail of Home Office proposals are not yet available, but here is much of what they will need to address:

How far are the police and agencies inhibited in carrying out investigations?

Current definitions within the Regulation of Investigatory Powers Act, 2000 (RIPA) of "communication data" and "content" for the purposes of interception [5]mean that a range of new and important Internet based services are semi-invisible as far as access to "communications data" is concerned.

The authorities are not limited in circumstances where they seek a warrant for *full interception*; however there are practical problems of dealing with encrypted material and turning raw intercepts into useful intelligence. Nothing the government has announced about its intentions to reform the law will address the issues of encrypted material and intelligence assessment. Intercept material – content - is currently inadmissible[6].

Over the last 12 to 13 years, the period during which the new and important Internet based services have appeared, changes and improvements in other forms of technology have significantly extended and improved the range of facilities in the form of "digital footprints" available to investigators. These include better coverage of the movements of cellphone users (so long as the phone is simply switched on – this is known as cell site analysis), automatic number plate recognition, better quality and wider availability of closed circuit television, more extensive use of computer forensics (based partly on greater public use of computers), the ability to track Oyster card owner movements, a stronger ability to monitor financial transactions, and subscriptions to many more detailed commercial databases covering customer credit and purchase patterns[7].

Is it feasible to separate communications data from content?

[5] S 21: "lawful acquisition and disclosure of communications data", S 1 "unlawful interception
[6] S 17, RIPA
[7] eg http://www.marketingguru.co.uk/, experian, http://www.graydon.co.uk/

Every policy statement and press briefing suggests that the Home Office asserts that all that is needed is a redefinition of the terms within RIPA. Any legislation that goes through Parliament must end up with definitions which can be clearly understood and interpreted by the Agencies, the police, Internet Service Providers and the courts; the actual structure of new legislation will probably consist of primary law plus Codes of Practice.

In traditional analogue telephony, "comms data" is the detailed phone bill: who called whom, when, and for how long. Comms data from a cellphone company will additionally include information identifying the handset, the SIM and the location of the cell site to which a phone is at any one time registered. "Content" is what is said on each occasion, typically collected via audio recorder. On the Internet everything travels by data packets which often contain both "comms data" and "content". The packets have to be examined - "inspected" - to see what is going on. The legal definitions of "communications data" and "content" need to be converted into technical instructions – "filters" - which can be applied at very high speed and very reliably by specialist hardware called deep packet inspection devices (DPI).

Under current legal definitions "communications data" cannot include the contents of a webpage for example. With webmail a webpage will have elements which are "communications data" (who sent an e-mail and when) but also "content" (the subject matter and the message itself). However even if one were to change the definition there would still be the problem of separating out the material on the individual webpage – and that presents profound if not impossible challenges given the large number of different designs for webpages which simply deliver webmail. This generic problem of having to understand very large numbers of different webpage designs for webmail, instant messaging, bulletin boards, social networking, etc means that the range of filters which the DPI devices will have to handle will be vast and ever-changing. This is not the end of the matter, there are several different *underlying technologies* for instant messaging, internet telephony, multiple-player games etc, all of which will require their own filters. Social networking such as Facebook, LinkedIn, Google, MSN/Live, etc consist of *bundles* of ever-changing technical services and protocols; again, more filters will be required.

Yet further difficulties occur when trying to separate comms data within "apps", mini-programs as used on smartphones, tablets and new computer operating systems, and in the near future on games consoles and "smart" tvs.

Thus the costs of implementing the proposals of the CCDP consists partly of the hardware required but also the ongoing costs of managing and researching the range of filters.

One has to conclude that it is no longer practical to separate out communications data from content.

Will the CCDP be effective and provide value for money?

An increasing number of routine web-based services are now delivered in encrypted form using *https*, the same technology that is used to protect commercial

transactions. Companies are using this technology to protect their customers from routine eavesdropping; examples include most forms of web mail, social networking sites such as Facebook and the various services offered by Google – search, cloud-based documents, calendars, gmail, etc. DPI technology cannot routinely overcome this.

In addition the following techniques for evading scrutiny require no skill on the part of the user, simply the knowledge that such routes exist: the pay as you go data SIM used with a laptop, smart phone or tablet; the Internet Café; hijacking an unprotected Wi-Fi Internet access point,; acquiring a "free" e-mail address for which authenticated information is not required and then using that e-mail address to provide credentials for other services (credential laundering). Further concealment methods are available to those with some technological proficiency – much guidance is freely available on the web.

There is a further problem facing any forms of electronic intelligence gathering: while collection is easy the subsequent analysis to provide useful intelligence and to avoid the twin problems of false-positives (the software tells you to worry when you shouldn't) and false negatives) (the software fails to tell you when to worry) remains difficult. "Data mining" is the description of an ambition, not a fully working and reliable product.

On the question of value for money, a view must be taken of CCDP alongside all the other techniques, old and new, available to investigators. The costs of CCDP could easily be taking funds away from traditional investigations, regular well-established human-based surveillance techniques and the work of intelligence analysts. One must also worry that costs can easily run out of control. There will be a cloak of secrecy around any expenditure because of "national security" concerns, the contracts will probably be shrouded in commercial confidentiality, and as can be seen from the analysis so far it is highly likely that it will suffer from a lack of clarity in specification, requiring significant additional expenditure as "on-costs". This has been the definitive recipe for hitting the taxpayer with gross cost overruns.

Are there alternative legislative proposals which might be more productive?

One route to consider is aiming legislation not at Internet Service Providers (whose main role is to deliver the Internet to homes and offices) but to those offering substantial services and asking for an interception capability on the analogy of that currently in place in section 12 of RIPA. This route is being pursued in the US.[8] The difficulty here is that although the UK Parliament can pass such legislation empowering a Secretary of State to issue orders, it would only be enforceable against UK businesses and the vast majority of services in which investigators have an interest are outside the jurisdiction. One would need the voluntary cooperation of the owners of such services – and even where these are identifiable there would be profound commercial and political implications for such service providers particularly if they are asked to carry out what might be potentially a whole

[8] http://www.nytimes.com/2010/09/27/us/27wiretap.html?pagewanted=all; an extension to CALEA, Communications Assistance for Law Enforcement Act, 1994

population surveillance exercise as opposed to more limited operations which had been scrutinised and approved by a court.

More radical forms of legislation would almost certainly have *to abandon the attempt to separate comms data from content*, so that a **monitoring warrant** would cover both. This would mean that the peculiar UK position of making intercept evidence inadmissible[9] would also have to be abandoned. Any new power along these lines would almost certainly have to subject to judicial scrutiny as opposed to the current position where warrants are issued, for historic reasons, by a Secretary of State acting on behalf the Crown.

One can envisage a low level warrant or authorisation asking ISPs and telephone companies to produce their **existing records** corresponding to communications data – this would be very similar to the current position. One might include a "data retention" element, as now.

One can also envisage a new type of warrant, also issued by a judge, on the basis that although an individual who is not currently presenting sufficient of a threat to justify full scale monitoring there was the possibility by virtue of people whom they knew or views they were thought to hold, it might be useful if the ISP were to **retain** their communications and content for a period of year against the future possibility that the police or other investigators produced a full warrant to view the material. This would address a problem identified by investigators that on occasion they identify a substantial conspiracy in an advanced stage and wish to know something of the previous actions and thoughts and associates of those thought to be involved. (This is the argument advanced for data retention). However this last proposal has many difficulties associated with it – what would be the actual criteria for the issuing of such a warrant and how would it be supervised? But it would have the further advantage of being targeted – effort and expenditure would be directed against those who might in the future be of interest, as opposed to the 99.5% of the population who never will be.

[9] S 17 RIPA