BIG BROTHER WATCH
DEFENDING CIVIL LIBERTIES, PROTECTING PRIVACY

INVESTIGATORY POWERS REPORTS BRIEFING

David Anderson's report *A Question of Trust* was published on the 11th June 2015 having been commissioned under the Data Retention and Investigatory Powers Act 2014 (DRIPA) s7. In his role as the Independent Reviewer of Terrorism Legislation, Anderson was required to examine:

(a) the threats to the United Kingdom,
(b) the capabilities required to combat those threats,
(c) the safeguards to protect privacy,
(d) the challenges of changing technologies, and
(e) the issues relating to transparency and oversight.[1]

The Intelligence and Security Committee published its report *Privacy and Security: A Modern and Transparent Legal Framework* on the 12th March 2015. The report presents a review of the full range of intrusive capabilities available to the UK intelligence Agencies.[2]

A third report on the use of intrusive powers, commissioned by the former Deputy Prime Minister Nick Clegg and conducted by the **Royal United Services Institute** has yet to be published.

The Home Secretary has stated that it is likely that the recommendations and findings of the three reports will form the basis of the **Investigatory Powers Bill**, set to be published in the Autumn.

This briefing provides:

[1] https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf

[2] https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20150312_ISC_P%2BS%2BRpt%28web%29.pdf?attachauth=ANoY7crKxKFzNbeQlNEOOmMzmWw_lp3Q9sTaqoOUMTBgMChLzWT80tH7NaPMT66Hweq3HiaAgKPpX-QIpcD5wA7fwEeUetdoH95qr5qcoCuXL_a-g9mZ0LztftSwjqHkh-67oruiLRMhoGYpdn-bHW3_UqdgRuZqmHCzBljjvA-uowNBpwzGc_j6rHxsBM-dFR6MNZICseBp1lVO3av4q6KSNbW6Pg_pHsmAF5UUPBTT8hq5YNDvnzzgsZliZ_JchX5U4ubl_dE9&attredirects=0

www.bigbrotherwatch.org.uk
55 Tufton Street, London, SW1P 3QL
0207 340 6030 I info@bigbrotherwatch.org.uk

BIG BROTHER WATCH
DEFENDING CIVIL LIBERTIES, PROTECTING PRIVACY

ANDERSON AND THE ISC: SIMILARITIES AND DIFFERENCES

Legislation

The reports both call for new legislation, however they differ on the approach to be taken.

The ISC recommended the creation of an Intelligence Services Bill, which would provide separate legislation for the security agencies from public authorities and law enforcement. This proposal would see MI5, MI6 and GCHQ adhere to one piece of legislation, rather than the numerous pieces of legislation noted below:[3]

- Security Service Act 1989;
- Intelligence Services Act 1994;
- Regulation of Investigatory Powers Act 2000;
- Wireless Telegraphy Act 2006;
- Telecommunications Act 1984;
- Counter-Terrorism Act 2008.

The ISC also highlighted a number of changes that need to be made, including:

- The need for agencies to have an "*interception warrant in place before seeking communications from a foreign country*"[4]
- More clarity given to the exchange of "*raw intercept material with international partners*"[5]
- A consideration for the statutory protection of "*sensitive professions*"[6]; and
- More clarity for the capabilities and safeguards granted under Section 1984 of the Telecommunications Act 1984.[7]

Anderson takes a broadly different view, arguing for a single, unified Bill to cover surveillance powers; regardless of which organisation is using them. The proposed Bill would combine sections from a number of acts, including RIPA part 1, The Data Retention and Investigatory Powers Act 2014 and The Counter Terrorism and Security Act 2014 Part III. The acquisition and use of bulk personal data would be covered by this Bill.

Anderson is careful to stipulate that the new legislation should *"repeal or prohibit the use of any other powers providing for interference with communications".*[8]

[3] Recommendation XX
[4] Recommendation SS
[5] Recommendation TT
[6] Recommendation UU
[7] Recommendation SS
[8] P.826

www.bigbrotherwatch.org.uk
55 Tufton Street, London, SW1P 3QL
0207 340 6030 I info@bigbrotherwatch.org.uk

In keeping with his emphasis on clarity and transparency, Anderson recommended that the new law should define the "*possible powers and safeguards*" governing the receipt and sharing of intercepted material to and from international partners. There is also a call for the Bill to be worded in non-technical and easily understandable language.[9]

The Commissioner System

Both the ISC and Anderson recognised the need for some element of reform of the Commissioner system; however they differ on both scale and direction of the change.

The ISC prioritised the issues of resourcing and staffing in Commissioner's offices. They recommend a sharing of resources across the *"different parts of the oversight structure"*[10] including the Commissioners, Intelligence and Security Committee and the IPT.

They highlighted that parts of the Commissioners' responsibilities existed on a non-statutory footing because of their "piecemeal" development.[11] The ISC argued for an increased role for the Commissioners, for example in scrutinising internal sign-offs.[12]

Anderson on the other hand favoured a radical change in the way the Commissioner system operates. He recommended the creation of a new body, to be called the Independent Surveillance and Intelligence Commissioner (ISIC). He envisages this as being a "*well-resourced and outward-facing regulator*". The body would merge the Intelligence Services Commissioner, the Interception of Communications Commissioner and the Office of Surveillance Commissioners to create a body which would be responsible for the judicial authorisation of all warrants and of certain categories of requests for communications data.

Judicial Oversight

The main area of disagreement between the two reports is in the role of the judiciary in the authorisation of surveillance warrants.

In its report **the ISC** repeatedly argued that the "*most intrusive activities must always be authorised by a Secretary of State*".[13] In the ISC's view, Ministers *"are able to take into account the wider context of each warrant application and the risks involved".*[14] Additionally they argue that as Ministers are democratically accountable they were the ones who should justify the issuing of warrants.[15]

[9] P.286
[10] Paragraph 211, ISC report
[11] Recommendation JJ
[12] Recommendation KK
[13] Recommendation ZZa
[14] Recommendation FF
[15] Recommendation FF

www.bigbrotherwatch.org.uk
55 Tufton Street, London, SW1P 3QL
0207 340 6030 I info@bigbrotherwatch.org.uk

Looking at capabilities *"which fall below the threshold requiring a warrant"* the ISC found that this was generally acceptable, but recommended a *"clear line of separation"* between the investigative and authorising teams.[16] Additionally the ISC pushed for "*greater retrospective review*" by the Commissioners.

Anderson argued that "*specific interception warrants, combined warrants, bulk interception warrants and bulk communications data warrants*" should be signed off by a Judicial Commissioner.[17] At present the process of signing off on interception warrants is the role of a Secretary of State. Anderson questions whether this is the *"best use of the Secretary of State's valuable time"* (in 2014, 2,795 warrants were authorised by a Secretary of State). By imposing judicial authorisation as the final step of the warrant process Anderson argued, that it would "*improve public confidence in the system"* and lead to better cooperation with US technology firms which are used to dealing with a judicial system domestically. It is worth noting that the issuing of judicial warrants when the police undertake property interference, intrusive surveillance and long-term undercover operations is well established.

The **two reports do agree** that law enforcement applications for Communications Data should be signed off internally, using the Designated Person (DP) and SPoC system. Anderson stated that unless the warrant requires bulk data it "*should be issued only on the authority of a DP authorised to do so by the authorising body*".[18] Additionally Anderson saw the proposed ISIC as having a role in authorising Communications Data requests when they are "*novel or contentious*".

Looking specifically at the acquisition and use of Communications Data by local authorities, Anderson concluded that the current requirement for them to apply to a Magistrate should be lifted. Instead he proposed they utilise the SPoC system provided by the National Anti-Fraud Network.[19]

The Investigatory Powers Tribunal (IPT)

The IPT didn't form a major part of the **ISC's report** and only one recommendation was made, focusing on the fact that there was no mechanism to appeal a ruling domestically. The Committee recognised the importance of a "*domestic right of appeal and recommend that this is addressed in any new legislation*".[20]

Anderson looked in more depth at the IPT and made a number of recommendations to increase its remit and improve its impact. For instance, Anderson argued that the Communications Service Providers, when they are at fault, should be subject to its rulings. He also advocated that the ISIC (if created, the current organisations if not) should be permitted to inform subjects of any wrongful surveillance.

[16] Recommendation HH
[17] P.289
[18] P.289
[19] P.297
[20] Recommendation LL

www.bigbrotherwatch.org.uk
55 Tufton Street, London, SW1P 3QL
0207 340 6030 I info@bigbrotherwatch.org.uk

Anderson's third recommendation echoes the ISC, arguing that there should be a right to appeal within the UK. He also considered that it may be useful to give the court the ability to rule on the compatibility of UK legislation with the ECHR.

Definitions of Communications Data

The ISC felt that communications data can play a useful role in the investigation of crime. However they also pointed out that some elements *"have the potential to reveal details about a person's private life that are more intrusive".* Examples of "intrusive" communications data would be details of websites visited *or the location tracking information in a smartphone.* As a result they argued for the creation of a new structure for this data:

- **Communications Data** -The numbers and date/time of a call.
- **Communications Data Plus** - personal or organisational details which could be intrusive. This would be subject to stricter safeguards.
- **Content-Derived Information** -The accent of an individual speaking. Would be treated with the same safeguards as content.

Anderson didn't go as far as to suggest new definitions, instead recommending a review of the current ones. He was particularly keen to point out that any review should be as "*open and inclusive*" as possible.

Draft Communications Data Bill

The **ISC** report barely touched upon the Draft Communications Data Bill, stating only that access to Communications Data was a crucial capability for both the intelligence and law enforcement agencies.

Anderson went into far more depth. On the issue of web logs (defined as a record of the websites visited up to the first '/' of its url for example www.google.com or www.bbc.co.uk) which the Home Office called fervently for in the Draft Bill, he acknowledged that they may be useful but that he is *"not aware of other European or Commonwealth countries in which service providers are compelled to retain their customers' web logs for inspection by law enforcement."*

He went on to say that he was *"not presented with a detailed or unified case"* to require the retention of web log data. More information was needed on why the data would be needed, what the current gaps were, what the privacy implications were and how the information would be securely stored.

Anderson 's views regarding the retention of third party information were similar in that he stated *"there should be no question of progressing this element of the old draft Bill until such time as a compelling operational case has been made"*

www.bigbrotherwatch.org.uk
55 Tufton Street, London, SW1P 3QL
0207 340 6030 I info@bigbrotherwatch.org.uk

Bulk Collection and Interception

Concerns around the collection of bulk data collection was one of the main issues that led to the ISC writing its report. It found that there was no evidence of the gathering of this data as being either indiscriminate or mass collection. The chapter concluded that the ISC was satisfied that "*current legislative arrangements and practice are designed to prevent innocent people's communications being read*." It further found that GCHQ's capabilities in this area were valuable to its function.

The ISC was also concerned by the 'internal v external' issue and to help resolve this it recommended that the Government publish a "*clear and comprehensive list of communications*" and which category they fell into.

Anderson's views on bulk interception stated that in light of the case studies he was shown – but which were redacted for public consumption – he felt that *"bulk interception, as it is currently practised, has a valuable role to play in protecting national security."* He went on however to stress that *"It does not of course follow that it is necessarily proportionate, which is for the courts to decide."*

He went on to suggest a number of potential improvements, for example the aforementioned oversight and authorisation changes; adding that only the heads of the agencies should be able to apply for a warrant.

One of the recommendations was to allow for the acquisition of Communications Data in bulk. This negates the need to apply for a bulk interception warrant, and would allow for greater protections for the individual.

He argued that greater transparency for the reasons behind a warrant should be provided when the warrant is applied for.

Finally he called for more clarity over the 'internal v external' nature of warrants and stated that the current definitions were outdated and should be redrawn to focus on the "*location of the individuals rather than the communications*".

With this in mind he suggested that bulk interception warrants (not necessarily bulk Communications Data warrants) should be targeted at individuals who were believed to be outside the UK at the time.

www.bigbrotherwatch.org.uk
55 Tufton Street, London, SW1P 3QL
0207 340 6030 I info@bigbrotherwatch.org.uk

ANDERSON REPORT: KEY ISSUES AND RECOMMENDATIONS

THE NEED FOR NEW LEGISLATION

The Threat in Perspective

Anderson noted that *"it is generally a mistake (though a surprisingly common one) to describe threat levels as "unprecedented". Two points need to be kept in mind:*

(a) Events capable of taking life on a massive scale are a feature of every age and every stage of development.
(b) Whilst some of the threats faced at any given time will be realised, others will not."[21]

He went on to say:

> *"The moral is not that threats ought to be ignored: on the contrary, any credible threat should be guarded against. The point is, rather, that claims of exceptional or unprecedented threat levels – particularly if relied upon for the purposes of curbing well-established liberties – should be approached with scepticism."*[22]

On the issue of National Security, he noted that it is *"nowhere defined in statute"*[23]. This is of huge concern as it enables legislation, which has multiple national security exemptions as part of the statutory safeguards, to define national security broadly.

The Regulation of Investigatory Powers Act 2000

Drafted before the vast uptake of the internet, the Regulation of Investigatory Powers Act 2000 (RIPA) has been controversial and accused of failing to keep up with the digital revolution. In his report, Anderson stated:

> *"RIPA, obscure since its inception, has been patched up so many times as to make it incomprehensible to all but a tiny band of initiates."*[24]

Going further, he said that *"this state of affairs is **undemocratic, unnecessary and – in the long run – intolerable**."*[25]

[21] P.39
[22] P.40
[23] P.41
[24] P.8
[25] P.8

www.bigbrotherwatch.org.uk
55 Tufton Street, London, SW1P 3QL
0207 340 6030 I info@bigbrotherwatch.org.uk

As a resolution, he recommended the introduction of an entirely comprehensive new law which should be drafted from scratch, replacing the multitude of current powers and providing for clear limits and safeguards:

- Affirmation of privacy of communications
- Prohibits interference with them by public authorities, save on terms specified,
- Provides judicial, regulatory and parliamentary mechanisms for authorisation, audit and oversight of such interferences.

He also made the case that any new legislation should be written (as far as possible) in *"non-technical language".*[26]

In the past, arguments have been made for further powers on the basis that they are being requested by law enforcement as a whole. Conversely, Anderson made the point that *"there has been no attempt to formulate uniform views within the law enforcement community, or to put such views across to me."*[27]

A Legislative solution

The debate concerning communications data capabilities may be organised under five overlapping heads: data retention, IP resolution, web logs/destination IP addresses, third party data and the search filter. Anderson summarised the position of law enforcement on each of these:[28]

- **Data retention**: Police and the CPS make the case that older data can be useful, giving examples of criminals being more guarded *"as the moment of a crime approaches"* and *"time lapse between the incident and the identification of a suspect will mean that old data is needed".*
- **IP address resolution**: In the Counter Terrorism and Security Act 2015 Part 3, Parliament extended the scope of compulsory data retention by service providers to include the data that are needed to link an IP address with the device that was using that address at a particular time. Law enforcement emphasised that it is no more than a stepping-stone. Some CSPs, particularly, those using dynamic IP addresses such as mobile phone operators, require destination IP as well as sender IP to match up who is involved in an action. There is the possibility that as the technology progresses with IPv6 (the latest version of the Internet Protocol), an IP address could potentially be assigned to a person rather than a property.

[26] P.285
[27] P.167
[28] P.174-179

www.bigbrotherwatch.org.uk
55 Tufton Street, London, SW1P 3QL
0207 340 6030 I info@bigbrotherwatch.org.uk

- **Web logs/destination IP**: Under this definition a web log would reveal that a user has visited e.g. www.google.com or www.bbc.co.uk, but not the specific page. Anderson stated that he was not aware of other European or Commonwealth countries in which service providers are compelled to retain their customers' web logs for inspection by law enforcement. The Communications Data Bill proposed the compulsory retention of web logs.
  On this point Anderson notes that it is widely accepted within the law enforcement community that:
  - the compulsory retention of web logs would be potentially intrusive;
  - the political environment (not to mention the legal environment: Digital Rights Ireland) may not be conducive to the imposition of such an extensive obligation; and that
  - there would be expense and complexity involved in making these changes (not least in terms of training staff within law enforcement), that would only be justified if any new power were to be extensively used.

The importance of trust

One of the key themes in the report is the need for public trust in the system. Anderson noted that the service providers put a huge amount of emphasis on the trust that their customers place in them.

The service providers see protecting their customers' privacy as a key element to maintaining that trust. Anderson noted that *"they stress the importance that they comply (and are seen to comply) not only with national law, but with internationally recognised principles of human rights."*.[29] However, for service providers operating internationally, complying with the law is a complex demand.

Anderson recognised that the service providers' view is that voluntary relationships, with the UK government and elsewhere, can no longer be the basis of surveillance. He quotes one company as saying that: *"We can't get into conversations that leave our customers on the outside….our priority is our brand, not UK intelligence."*[30]

Digital Rights Ireland

Anderson also drew attention to the EU's Data Retention Directive and the impact it has had on recent legislation in the UK. The judgment of the European Court of Justice (CJEU) in *Digital Rights Ireland,* in April 2014 was a successful challenge to the validity of the EU's Data Retention Directive.

The Directive required service providers to retain data generated for billing purposes concerning the use of telephone, internet and email services for between 6 and 24 months. The scope of the data was broad and included data necessary to identify a sender and recipient. Service providers would

[29] P.204
[30] P.206

www.bigbrotherwatch.org.uk
55 Tufton Street, London, SW1P 3QL
0207 340 6030 I info@bigbrotherwatch.org.uk

hold the data beyond the period of time when it might need them. The service provider was required to make data available, to the police and security services. The implementing legislation in the UK required service providers to keep that data for 12 months.

The CJEU declared the Directive to be invalid, for failure to comply with the principle of proportionality.

3 months later in July 2014 the UK Government rushed through the Data Retention and Investigatory Powers Act 2014 (DRIPA) which legislated that service providers had to continue to retain billing data for 12 months. Other European countries however followed the lead of the CJEU and allowed data retention to lapse. Bulgaria, Romania, Germany, Cyprus, Czech Republic all annulled data retention laws prior to the *Digital Rights Ireland* judgment. Austria, Slovenia and Romania were the first three to do so since the judgment.

Anderson has recommended that the system of retaining data under DRIPA should continue to exist and that it *"should be retained in a manner that is consistent"* with legal obligations.[31] He also noted that law enforcement supports the retention of data by CSPs (as permitted under DRIPA). There is an acceptance that the 12 month retention period is proportionate.

CAPABILITIES

In the report, Anderson made reference to a number of capabilities. Some have been discussed publicly at length, whilst little is known about others.

Draft Communications Data Bill (Snoopers Charter)

Anderson was clear that any draft of new legislation should make sure that a detailed operational case is made. He is also clear that a rigorous assessment should be conducted of, the lawfulness, likely effectiveness, intrusiveness and cost of requiring such data to be retained. The report highlights times in the past when this has not been the case including the calls for web logs and sharing retention of third party data. Anderson is very specific that there should be no question of progressing proposals before a compelling *"operational case"* has been made.

Anderson also recommended that Government should initiate early and intensive dialogue with law enforcement and CSPs in order to formulate an updated and coordinated position, informed by legal and technical advice, on the operational case for adding web logs (or the equivalent for non-web based OTT (over the top) applications) to the data categories currently specified in DRIPA.

[31] P.263

www.bigbrotherwatch.org.uk
55 Tufton Street, London, SW1P 3QL
0207 340 6030 I info@bigbrotherwatch.org.uk

Bulk Data Collection

One of the most controversial findings of Anderson's report was the recommendation that the capability of the security and intelligence agencies to practise bulk collection of intercepted material should be maintained.

Anderson acknowledged that there are several court cases taking place in the IPT and EUCJ which means that his recommendation is subject to the rulings of those courts.

Extraterritorial effect

In his report, Anderson stated that service providers operating in the UK should not need a license, and should not be required to store data in the UK. However, in order to address issues of accessing material from overseas service providers, the Government should:

- Seek the cooperation of overseas service providers,
- Seek the improvement and abbreviation of MLAT (Mutual Legal Assistance Treaty) procedures, and
- Take a lead in developing and negotiating a new international framework for data-sharing among like-minded democratic nations.

Home and Away

Anderson noted that *"for practical purposes"* any framework for the interception of external communications will have to be ECHR-compliant.[32] He also points out that this is difficult because:

> *"It is generally acknowledged to be impossible, when gathering communications between two individuals who are both outside the UK, to avoid collecting some communication that are internal, in the sense that they are both to and from individuals inside the British Islands."*[33]

Anderson also raised the jurisdictional issues that arise in relation to the extra-territorial application of national laws requiring overseas service providers to make data available (e.g. DRIPA 2014 s4), particularly where those laws come into conflict with data protection requirements in the foreign state. New international standards for privacy may therefore be required.

[32] P.80
[33] P.80

www.bigbrotherwatch.org.uk
55 Tufton Street, London, SW1P 3QL
0207 340 6030 I info@bigbrotherwatch.org.uk

Open Source Intelligence (OSINT)

Most social media is "open source", meaning anyone can access it. Twitter for example works on the principle that anyone can read a tweet unless the user chooses to protect it.
Anderson acknowledged that UK law enforcement and the security and intelligence agencies use OSINT, though the extent of that use is not publicly known.

New legislation should include OSINT, setting out when and how it should be used and by whom.

Encryption, Backdoors and Front Doors

Anderson acknowledged that encryption is a crucial part of the everyday transactions that we make with our banks, and is imperative to keeping financial data secure. Large technology companies are now making encryption a standard part of their technology and devices, with the onus being on the consumer to opt out of encryption rather than opt in. This is a trend that many companies are adopting. This is to counteract allegations that intelligence agencies from around the world have created back doors into their communications without permission or the understanding of the companies themselves.

In order to outline the issues and concerns regarding encryption and efforts to undermine encryption, Anderson quoted Bruce Schneier from the Office of the Director of National Intelligence, in the USA who stated:

> *"Cryptography forms the basis for online trust. By deliberately undermining online security in a short sighted effort to eavesdrop the NSA is undermining the very fabric of the internet."*[34]

Whilst Anderson notes the concerns amongst the intelligence agencies and law enforcement about the diminishing access to communications due to encryption, he also acknowledged that *"there are many strands to the encryption debate"* and that *"the experts to whom we spoke told us that if one government can gain access through a door, so can other governments and private actors."*[35]

Enforced decryption

Anderson explained the current situation regarding enforced decryption; where a relevant authority can demand the decryption key be handed over to enable all contents of an encrypted device to be examined. As Anderson states this power *"represents a possible way around the secure encryption of modern devices."*[36] Failure to comply with an enforced decryption request can result in a prison sentence.

[34] P.62
[35] P.61
[36] P.146

www.bigbrotherwatch.org.uk
55 Tufton Street, London, SW1P 3QL
0207 340 6030 I info@bigbrotherwatch.org.uk

Intrusive capabilities

As an alternative to creating back doors, Anderson suggested *"the use by governments of hacking capabilities and malware, often referred to as CNE [Computer Network Exploitation]".*[37]

Computer network exploitation (CNE)

CNE is better known as "hacking" and can include hacking into *"computers, servers, routers, laptops, mobile phones and other devices."*

However this has been controversial. Anderson acknowledged that hacking of private computers was made legal by the Government in March 2015, with no debate or discussion, by publishing a code of practice amending the Draft Equipment Interference Code.

Prior to that amendment, the Intelligence and Security Act 1994 s5 was the only piece of legislation which gave the Secretary of State the power to issue warrants authorising the agencies to interfere with property in quite general terms.

RIPA interception

RIPA is the primary means by which an interception may be authorised via a warrant. This is issued under RIPA s5 and signed by a Secretary of State who must believe that the warrant is necessary on grounds of *"national security, preventing or detecting serious crime, safeguarding the economic well-being of the UK or for the purpose of giving effect to an international agreement."*[38]

It is worth noting that with very few exceptions, material obtained under an interception warrant is not admissible as evidence in UK courts. Anderson recommended that the number exceptions when intercepted material can be used in court should be expanded.

Bulk interception

GCHQ provided both the ISC and Anderson with case studies to demonstrate the effectiveness of its bulk interception capabilities. In response Anderson stated that:

> *"They leave me in not the slightest doubt that bulk interception, as it is currently practised, has a valuable role to play in protecting national security. It does not of course follow that it is necessarily proportionate, which is for the courts to decide."*[39]

[37] P.63
[38] P.103
[39] P.130

www.bigbrotherwatch.org.uk
55 Tufton Street, London, SW1P 3QL
0207 340 6030 I info@bigbrotherwatch.org.uk

On the ISC report, Anderson notes that:

> *"There are limits to what the public will (or should) take on trust. It is unfortunate, therefore, that the examples that the ISC gave to demonstrate the effectiveness of GCHQ's bulk interception capabilities had to be redacted from the open version of its report."*[40]

Utility of intercept and communications data

Anderson noted that the ongoing view of the Government to not allow legal intercept as evidence in criminal proceedings is on the basis that the benefits are disproportionate to the "costs and risks".[41] Whilst this limitation is "*not within my remit to revisit"* places a *"premium on obtaining data by other means: e.g., by interrogating devices and by applications to a court for stored communications. Content of communications and communications data itself is frequently deployed as evidence, as indeed foreign intercept may be."*[42]

Targeted warrants

RIPA s8 distinguishes between two different kinds of warrant that may be granted. Warrants issued under s8(1) are targeted, as they must describe either *"one person as the interception subject"* or *"a single set of premises*" where the interception is to take place under ss8(1) and (2).[43]

Thematic Warrants

Thematic warrants are sometimes issued under s8(1), which cover *"any organisation or any association or combination of persons."*[44] This interpretation of s8(1) was first acknowledged in the ISC Privacy and Security Report in March 2015.

Internal v External

Warrants issued under s8(4), often termed "external" warrants; authorise interception of communications where one or both of the senders or recipients of a communication are located outside the British Islands. Section 8(4) warrants may be used to authorise the interception of all communications transmitted on a specified route or cable, or carried by a particular service provider.

[40] P.130
[41] P.168
[42] P.169
[43] P.104
[44] P.104

www.bigbrotherwatch.org.uk
55 Tufton Street, London, SW1P 3QL
0207 340 6030 I info@bigbrotherwatch.org.uk

The boundary between "internal" and "external" communications is not straightforward. The Office of Security and Counter Terrorism interpretation was, as set out in the Charles Farr's Statement (Director of the OSCT), that:[45]

(a) Two people in the UK who email each other are engaging in internal communication, even if they use an email service which is housed on a server in the United States. The fact that the communication travels via a server overseas does not make it external, but it may well be collected under a warrant targeting external communications.
(b) A person in the UK who communicates with a search engine overseas is communicating with a server overseas and engaging in an external communication. Likewise a person who posts a public message such as a tweet or Facebook status update, is sending an external communication unless all the recipients of that message are within the British Isles.

Farr's evidence was the first time this definition had been made publicly clear. Indeed Anderson acknowledged that some people have considered those distinctions counter-intuitive: for example, many people might not consider a Google search to be a communication at all, let alone an external communication.

The ISC report was clear that further clarity on "internal" and "external" is required.

Communications data and intelligence

Anderson noted that communications data allows for MI5 to "*build a picture of a subject of interest's activities*."[46] GCHQ also told Anderson that it "*makes extensive use of communications data to develop its intelligence picture, though much of its data is obtained as a by-product of its bulk interception of content.*"[47] GCHQ has established that they can analyse communications data to find patterns that reflect particular online behaviours.

These examples provided by Anderson show that communications data clearly provides a detailed and often intimate picture of an individual's life. Whilst the intelligence agencies state that this is currently used for counterterrorism, there is always the potential that it could be used for other purposes and applied as a broader scope of intelligence gathering.

Communications data and crime fighting

Evidence given by the National Crime Agency reveal that alongside their day to day work the use of communications data could be applied to preventing crime occurring rather than just investigating criminal acts. This poses a number of questions which need further exploration.

[45] P.108
[46] P.134
[47] P.134

www.bigbrotherwatch.org.uk
55 Tufton Street, London, SW1P 3QL
0207 340 6030 I info@bigbrotherwatch.org.uk

In the report, the NCA are quoted as saying that 90% of all serious crime investigations use communications data. The NCA state that with regards to online crime, communications data provides *"an opportunity for law enforcement to be proactive, looking for suspects, rather than waiting until a crime has been committed and a complaint made."*[48]

Anderson noted that:

> *"One particularly controversial aspect of communications data use is the compulsory retention by service providers of data, now enshrined in DRIPA 2014. Retained data provides information about conduct in the past, often before a suspect is identified. It is frequently relied on to piece together conspiracies and associations between groups of criminals."*[49]

Bulk personal datasets

Anderson acknowledged that "*the use by security and intelligence agencies of bulk personal datasets was publicly avowed only on 12 March 2015 when the ISC published its report."*[50] He goes on to acknowledge that he had been briefed on them well in advance of that report. The public however still know very little about what they are and how they are used. This remains a point of concern.

Anderson offers a little more information than the ISC, by stating that:

> "*The dealings of individuals with Government and non-governmental bodies are typically recorded in electronic databases. Those databases (which include passport application data) may be easily searched in order to obtain information about a particular individual or groups of individuals."*[51]

When aggregated, that data he states:

> *"it becomes a powerful tool in the hands of the security and intelligence agencies or investigators searching for suspect behaviour*."[52]

An example of HMRC's Connect database is provided, which is described as a *"high-tech analysis system"* which allows, when combined with a *"wide range of data sources",* the identification of *"evasion at the touch of a button"*[53].

[48] P.135
[49] P.135
[50] P.139
[51] P.145
[52] P.146
[53] P.146

www.bigbrotherwatch.org.uk
55 Tufton Street, London, SW1P 3QL
0207 340 6030 I info@bigbrotherwatch.org.uk

Five Eyes partners

The UK agencies, together with their counterparts in Australia, Canada, New Zealand and the USA, form part of the Five Eyes partnership.

Anderson made the important point that "*the precise boundaries between communications data and content are not defined in the same manner around the world*."[54] However, there is broad consensus that the content of a communication falls into a different category from communications data.

The UK is unique in the Five Eyes in making no use of judges for the prior authorisation of interception warrants. However there is no single standard applied by the other members.

Anderson explains that:

> *"law enforcement bodies in the United States, Canada, Australia and New Zealand must all obtain judicial authorisation before they carry out interception … In Canada and Australia, some form of judicial authorisation is required before the law enforcement can access communications data. In the USA, federal law enforcement agencies, e.g. the FBI, may access communications data without judicial authorisation, but State police ordinarily require a subpoena or a court order in order to do so."*[55]

Anderson noted that a brief review of the Five Eyes partners demonstrates that they all have at least some element of oversight by the legislature, as well as scrutiny by a Commissioner or Inspector-General.

MOVING FORWARD

Safeguards

Anderson recommended additional safeguard, including:

- judicial authorisation by the newly created Independent Surveillance and Intelligence Commission (ISIC);
- a tighter definition of the purposes for which it is sought, defined by operations or mission purposes;
- targeting at the communications of persons believed to be outside the UK at the time of those communications;

[54] P.148
[55] P.149

www.bigbrotherwatch.org.uk
55 Tufton Street, London, SW1P 3QL
0207 340 6030 I info@bigbrotherwatch.org.uk

- specific interception warrants to be judicially authorised if the applicant wishes to look at the communication of a person believed to be within the UK.[56]

One of the most high profile issues with the current surveillance regime is how those powers have been used to target legally privileged people (LPP) (lawyers, MPs, journalists). Anderson recommends that there should be special consideration for people who handle privileged or confidential information.

Whilst few people would argue against the principle that LPP should have explicit protections within surveillance legislation, there is a question why there should be additional, higher level safeguards for those members of society and not for the wider general public.

Authorisation and the ISIC

All warrants and certain categories of requests for communications data should be judicially authorised by a Judicial Commissioner at a new body: the Independent Surveillance and Intelligence Commission (ISIC). Anderson recommended that the Secretary of State should have the power to certify a national security warrant, but the Judicial Commissioner (a current or retired judge) would have the final say on issuing the warrant and can depart from it on the basis of the principles applicable in judicial review.

Big Brother Watch has called for judicial authorisation of the warrant process for a number of years. We wholly support this recommendation. One note of caution is that bearing in mind the varying quality of the current Commissioner's, it is imperative that the judge has the necessary technical and legal knowledge in this area.

Oversight and the ISIC

As well as an authorisation capacity, Anderson recommends that the ISIC should replace the offices of the three current Commissioners. The ISIC would take over the intelligence oversight and would be responsible for the judicial authorisation of all warrants and of certain categories of requests for communications data. Anderson is clear that it should be *"public-facing, transparent, accessible to media and willing to draw on expertise from different disciplines."*[57]

Oversight and the Investigatory Powers Tribunal (IPT)

The IPT has been subject to much criticism; notably that it fails to provide the necessary system of redress that members of the public need if they believe they have been a victim of unlawful surveillance.

[56] P.5
[57] P.8

www.bigbrotherwatch.org.uk
55 Tufton Street, London, SW1P 3QL
0207 340 6030 I info@bigbrotherwatch.org.uk

Anderson recommends that the IPT should be beefed up and that its rulings are subject to appeal on points of law.

How recommendations include, expanding the jurisdiction of the IPT be expanded to cover circumstances where it is the CSP at fault, rather than a public authority (intercepting the wrong communications and/or disclosing the wrong data).

Internal Authorisation

Law enforcement use two modes of internal authorisation for access to communications data – a Single Point of Contact (SPoC) and a Designated Person.

Anderson recommends placing the SPoC system on a statutory footing and making the Designated Persons independent from operations and investigations. Anderson hopes that this recommendation will lead to an authorisation system that the public can have faith.

Law enforcement gave their *"unanimous support"* for the SPoC arrangements.[58] Anderson notes that there is less enthusiasm for the introduction of magistrate authorisation which is now required for local authorities. The magistrate system has been widely criticised by the IOCCO and OSC.

Interestingly, law enforcement provided no comment to Anderson on the systems for parliamentary control or judicial oversight.

Intelligence and Security Committee (ISC)

Anderson recommends that the Intelligence and Security Committee (ISC) should continue *"not only because parliamentary oversight is desirable in principle but because of the knowledge and understanding that its members bring to parliamentary debates with nationals security implications."*[59]

However, he also recommends that the roles of the proposed ISIC and the ISC should not overlap, especially with regard to reporting functions and resources. He states that Parliament needs to consider whether:

- the Chair should be a member of the opposition party, rather than appointed by the Prime Minister
- the ISC's investigative resource in due course to the ISIC
- the ISC should be a full Select Committee (perhaps merged with the Defence Select Committee). This would mean the members are elected and to which the ISIC would report where necessary in closed session.

[58] P.167
[59] P.306

www.bigbrotherwatch.org.uk
55 Tufton Street, London, SW1P 3QL
0207 340 6030 I info@bigbrotherwatch.org.uk

Transparency

Anderson recommends that consideration is given to how Parliament and the public can be better informed about why they need their powers, how they interpret those powers, the broad ways in which those powers are used and why any additional capabilities might be required.

Anderson notes that public authorities *"should contribute to any consultations on the new law, so as to ensure that policy-making is informed by the best evidence."*[60]

Service Providers Recommendations

A number of specific suggestions emerged from the special meeting of the Communications Data Steering Group, where the companies and law enforcement and worked together. These were:

(a) Data that does not originate or terminate on the CSPs' network should be considered "third party data", not for the CSP to store and disclose.
(b) Consideration should be given to limiting disclosure of retained communications data in civil cases where that goes beyond the purposes for which the data had been retained.
(c) Legislation should require continued consultation between law enforcement and CSPs, so as to ensure that law enforcement can obtain the necessary information by the most effective means, without dictating the precise methods to be used by CSPs to produce it.
(d) Communications data should be redefined to include user data on the one hand and use data on the other, to create a simple and transparent division between the person who is accessing the internet or making a communication and the usage data which is inherently more private and would detail and individuals' activities.
(e) Content should be defined, so as to ensure there is no ambiguity over their obligations to produce material, particularly when stored in the cloud.[61]

[60] P.306
[61] P.212

www.bigbrotherwatch.org.uk
55 Tufton Street, London, SW1P 3QL
0207 340 6030 I info@bigbrotherwatch.org.uk

Big Brother Watch Policy Recommendations

There are a number of recommendations which feature in Anderson's report that Big Brother Watch has called for, either directly in our submission to the report, or in submissions to other inquiries, including that of the ISC.

Judicial Authorisation

Recommendation:

A new requirement of judicial authorisation (by Judicial Commissioner) of all warrants for interception, the role of the Secretary of State being limited to certifying that certain warrants are required in the interests of national security relating to the defence or foreign policy of the UK

Big Brother Watch: In our submission to David Anderson recommended that:

1. One element that is almost entirely missing from UK surveillance oversight is judicial oversight. Apart from the authorisation of RIPA warrants at a local government level, there is no input from judges. This is something that should be rectified.

2. Ideally this process would include high level judicial authorisation for techniques such as:
    a. Interception warrants.
    b. Directed surveillance warrants.
    c. The use of Covert Human Intelligence Sources (with regard to undercover operatives).
    d. Intrusive surveillance.
    e. Certified warrants not relating to an individual.

3. As well as this it would be useful for low level judicial authorisation to be introduced for the acquisition of communications data. As has been raised in the recent Office of Surveillance Commissioners annual report, there may be an issue with the level of technical expertise that is available in a Magistrates Court.[62]

4. To this end we repeat the calls made in our evidence to the Joint Committee on the Draft Communications Data Bill, that a central judicial authority should be established to allow the fast and efficient resolution of requests.

5. The lack of judicial authorisation in the UK is something that was addressed in the 2013 report of the UN's Special Rapporteur on the promotion and protection of freedom of opinion and expression.

6. The report warned that not including this kind of authorisation could lead to surveillance being authorised on a "*broad and indiscriminate basis, without the need for law enforcement authorities to establish the factual basis for the surveillance on a case-by-case basis*."

[62] Office of Surveillance Commissioners Annual Report for 2013-14 https://osc.independent.gov.uk/wp-content/uploads/2014/09/Annual-Report-of-the-Chief-Surveillance-Commissioner-for-2013-2014-laid-4-September-2014.pdf

www.bigbrotherwatch.org.uk
55 Tufton Street, London, SW1P 3QL
0207 340 6030 I info@bigbrotherwatch.org.uk

In the recommendations it was noted that communications surveillance should only take place "*under the supervision of an independent judicial authority*."[63] [64]

Oversight (the commissioner system and the IPT)

Recommendation:

1. Replace the three existing Commissioners' offices by the Independent Surveillance and Intelligence Commission (ISIC): a new powerful, public facing and interdisciplinary intelligence and surveillance auditor and regulator whose judicial commissioners would take over responsibility for issuing warrants, for authorising novel, contentious and sensitive requests for communications data and for issuing guidance.

2. Expanded jurisdiction for the Investigatory Powers Tribunal and a right to apply for permission to appeal its rulings.

Big Brother Watch: In our submission to David Anderson recommended that:

1. Turning to the Commissioner system it is clear that this too is in need of reform. The main problem is that although it ostensibly exists to ensure that the public are protected from wrongful or over-zealous intrusions into their lives, a large proportion of the public have little or no idea who the Commissioners are or what they do. This is a situation that needs to change; it should be the duty of each Commissioner to make every effort to properly communicate their work and their findings to the public.

2. All Commissioners should be made into full time posts and their staffing and funding levels should be increased to reflect the jobs that they have to do.

3. One element that is almost entirely missing from UK surveillance oversight is judicial oversight. Apart from the authorisation of RIPA warrants at a local government level, there is no input from judges. This is something that should be rectified.

4. One final part of the oversight system that should be discussed is the Investigatory Powers Tribunal (IPT). It has failed to provide the necessary system of redress that members of the public need if they believe that they have "*been a victim of unlawful action under RIPA*."

5. The IPT should not hold proceedings behind closed doors. Instead, cases should be brought in an open court, subject to a closed material procedure or public interest immunity framework. This would provide a greater level of transparency on the workings of the Tribunal, whilst also allowing for secrecy where necessary. Linked to this determinations on the facts of the case should always be made public, subject to the necessary technical and operational redactions.

[63] United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue* (2013), p. 14: http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf
[64] Ibid p. 21

www.bigbrotherwatch.org.uk
55 Tufton Street, London, SW1P 3QL
0207 340 6030 I info@bigbrotherwatch.org.uk