BIG BROTHER WATCH
DEFENDING CIVIL LIBERTIES, PROTECTING PRIVACY

Joint Committee on the Draft Investigatory Powers Bill - Written Evidence

December 2015

About Big Brother Watch

Big Brother Watch is a civil liberties and privacy campaign group founded in 2009. We produce unique research which exposes the erosion of civil liberties in the UK, looks at the dramatic expansion of surveillance powers, the growth of the database state and the misuse of personal information.

Specific to this process we campaigned against the Data Retention and Investigatory Powers Act 2014 and gave both written and oral evidence to the Joint Committee on the draft Communications Data Bill. We have also called for the reform of RIPA for a number of years.

Key Points

- **The 'double-lock' system is not judicial authorisation and needs more work.**
- **A proper system of redress needs to be implemented to help protect citizens from unlawful surveillance.**
- **Encryption must be protected.**

Summary

This response will focus on ten areas which we believe need further scrutiny before any further Bill is published:

1. Judicial Authorisation
2. Communications Data
3. Internet Connection Records
4. Bulk Powers
5. Equipment Interference
6. Encryption
7. The Commissioner System
8. Interception
9. Redress/User Notification
10. Terminology

Initially we would like to raise concern about the time given for scrutiny, in particular the time given to the Joint Committee. By our estimation, excluding the period when the two Houses are not sitting, the Committee will have had only seven weeks to scrutinise the draft Bill, a document which runs to 296 pages and rewrites a key part of the surveillance capabilities of a number of Government bodies. When you compare this with the five months given to the Joint Committee for the draft Communications Data Bill for scrutiny of a 118 page document it is clear that the promise of full scrutiny given by the Government is, at best, lacking.[1]

Response

Judicial Authorisation

When the draft Investigatory Powers Bill was published the Home Secretary promised "*stringent safeguards and robust oversight, including 'double-lock' authorisation*" claiming that this would establish a "*world-leading oversight*" regime.[2] However the system which has been put forward to ensure the intrusive powers are used properly, is anything but world leading.

The much vaunted 'double-lock' authorisation system, which the Home Secretary claims would see "*the most intrusive powers*" subject to "*approval by a judge as well as by the Secretary of State*" does not, on reading of the draft Bill, provide a double lock, rather a process of "review" from a politically appointed Judicial Commissioner. Without a proper system of authorisation and oversight there can be no confidence that any of the powers will be used proportionately.[3]

In the past a wide range of individuals and organisations, for example the Joint Committee on Human Rights[4], the House of Lords Constitution Committee[5], General Michael Hayden, former Director of both the CIA and NSA[6] and the Chair of the Intelligence and Security Committee Rt. Hon Dominic Grieve MP[7], have called for an end to the ministerial authorisation of warrants and the introduction of judicial authorisation, their arguments have been based on the following:

---

[1] *Draft Communications Data Bill*, June 2012: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228824/8359.pdf
[2] T. May, *Home Secretary introduces draft Investigatory Powers Bill*, 4th November 2015: https://www.gov.uk/government/news/home-secretary-introduces-draft-investigatory-powers-bill
[3] Ibid: https://www.gov.uk/government/news/home-secretary-introduces-draft-investigatory-powers-bill
[4] Joint Committee on Human Rights, Counter-Terrorism Policy and Human Rights: 28 days, intercept and post-charge questioning, September 2007, p. 9: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/243174/7215.pdf
[5] House of Lords Committee on the Constitution, Surveillance: Citizens and the state, 6th February 2009, p. 39: http://www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/18.pdf
[6] M. Hayden, Edward Snowden: Spies and the Law, 5th October 2015: http://www.bbc.co.uk/iplayer/episode/b06h7j3b/panorama-edward-snowden-spies-and-the-law
[7] D. Grieve, HC Deb, 25 June 2015, c1092, 25th June 2015: http://www.publications.parliament.uk/pa/cm201516/cmhansrd/cm150625/debtext/150625-0002.htm#150625-0002.htm_spnew140

1. The practicalities of a Secretary of State spending large amounts of time scrutinising warrants.
2. That no Secretary of State has ever explained their actions in relation to a warrant before Parliament, posing the question of strength of democratic accountability.
3. That independent judicial authorisation would harmonise us with other nations and would encourage service providers to work more closely with the agencies.

The proposed "double lock" system of political authorisation with judicial review fails to address any of these concerns.

Under **Sub-Clause 19(1)**, of the draft Bill it states that *"In deciding whether to approve a person's decision to issue a warrant under this Chapter, a Judicial Commissioner must review the person's conclusions as to the following matters".*

By asking the Judicial Commission to approve an existing decision using a method of review, relegates the Judicial Commissioner to little more than a rubber stamp, not the much vaunted "double lock".

The lack of power of the Judicial Commissioners is further emphasised at **Sub-Clause 19(5)** *"Where a Judicial Commissioner, other than the Investigatory Power Commissioner, refuses to approve a decision to issue a warrant... the person who made that decision may ask the Investigatory Powers Commissioner to decide whether to approve the decision to issue the warrant."*

Concerns about the proposed "double lock" have been raised by the Shadow Home Secretary, Rt Hon. Andy Burnham MP who wrote to the Home Secretary raising his concerns and the former Shadow Home Secretary Rt Hon. David Davis MP.[8] [9]

Effectively maintaining the current system with an extra process of review, does little to address the problems the warrantry process currently faces.

Secretaries of State will, under these proposals, continue to play a major role in scrutinising warrants. A process which may be simply unsustainable particularly when you consider that in 2014 alone the Home Secretary signed off 2,345 interception warrants, equivalent to 6 every day.[10]

The demand on time has been referred to be the **former Home Secretary, David Blunkett**:

> "*My whole world was collapsing around me. I was under the most horrendous pressure. I was barely sleeping, and yet I was being asked to sign government warrants in the middle of the night. My physical and emotional health had cracked*."[11]

---

[8] Guardian, *Andy Burnham calls for more judicial safeguards in the UK surveillance bill*, 9th November 2015: http://www.theguardian.com/politics/2015/nov/09/andy-burnham-investigatory-powers-bill-judicial-safeguards-letter-theresa-may

[9] Financial Times, *UK government's missed chance to fix broken surveillance system*, 6th November 2015: http://www.ft.com/cms/s/0/c7594530-83d6-11e5-8e80-1574112844fd.html#axzz3tA89DpBK

[10] D. Anderson, *A Question of Trust: Report of the Investigatory Powers Review*, p. 131, 11th June, 2015: https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Web-Accessible1.pdf

Martin Chamberlain QC has pointed out that the combination of the large number of warrants and the varied responsibilities of a Secretary of State are not suited to providing proper scrutiny;

> "*The idea that the decision maker can apply her mind properly to every one of these* [warrants] *is far-fetched*".[12]

In an age when we must all have a digital presence to exist. With society becoming increasingly dominated by technology and data and with the Internet of Things beginning to encroach on all our lives; the sheer wealth of data which will be produced will be staggering. The impact this will have on the warrantry process should be explored further, as the proposed system may be creating an obligation which a Secretary of State will struggle to maintain.

Unless there is a re-evaluation of these proposals there is a real risk that the general public will have little faith that full, proper, independent safeguards will be in place to keep them safe.

Internet Connection Records

Internet Connection Records (ICRs) are the one new power in the draft Bill. They are defined on the Home Office factsheet as being "*records of the internet services that have been accessed by a device*" but which "*do not reveal every web page that a person has visited or any action carried out on that webpage.*"

The Home Secretary has stated that this data is "*the internet equivalent of a phone bill*";[13] however this is not entirely accurate. A telephone bill reveals who you have been speaking to, when and for how long. Your internet activity on the other hand reveals every single thing you do online.

Analysing our internet history or what sites we have visited can provide a rich source of extremely revealing data which can be used to profile or create assumptions about an individual's life, connections and behaviour.

This is not the first time retention of this kind of data has been proposed. The draft Communications Data Bill proposed the retention of weblogs.[14] The Joint Committee who scrutinised that draft Bill determined that such proposals would creating a "*honeypot for casual hackers, blackmailers, criminals large and small from around the world and foreign states*"[15].

---

[11] Guardian, *Blunkett: how I cracked under the strain of scandal*, 7th October 2006: http://www.theguardian.com/politics/2006/oct/07/uk.davidblunkett
[12] Guardian, *Specialist judges should oversee snooping warrants, says leading warrants*, 19th October 2015: http://www.theguardian.com/world/2015/oct/19/leading-lawyer-calls-specialist-judges-oversee-snooping-warrants
[13] Home Office, *Home Secretary introduces draft Investigatory Powers Bill*, 4th November 2015: https://www.gov.uk/government/news/home-secretary-introduces-draft-investigatory-powers-bill
[14] Clause 1, *Draft Communications Data Bill*, June 2012, p. 13: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228824/8359.pdf
[15] Guardian, *MPs call communications data bill 'honeypot for hackers and criminals'*, 31st December 2012: http://www.theguardian.com/technology/2012/oct/31/communications-data-bill-honeypot-hackers-criminals

In their final report the same Joint Committee noted that:

> "*storing web log data, however securely, carries the possible risk that it may be hacked into or may fall accidentally into the wrong hands, and that, if this were to happen, potentially damaging inferences about people's interests or activities could be drawn.*"[16]

In light of this, if the Government wants the power of internet connection records they must explain clearly how they intend to safeguard the privacy of citizens first. They must also be 100% clear on how the technology will work.

Many technologists have expressed concern that the proposals in the draft Bill are not as straightforward as proposed. For example, concerns have been raised about how feasible it will be to separate the content of a message from an ICR.

In his evidence to the Science and Technology Select Committee **John Shaw, Vice President, Project Management at Sophos,** stated that in reality the line between content and communications data was "*incredibly blurred*".[17]

In written evidence to the same committee the **IT-Political Association of Denmark** raised further concerns about the viability of using ICRs in law enforcement investigations:

> "*Device identification seems to be the primary objective of ICRs, but there are limits as to what devices an ISP can actually identify. In general, the ISP can only identify devices that are connected directly to the ISP."*

It should be noted that Denmark had previously implemented a data retention scheme similar to the system proposed in the draft bill, these measures where repealed by the Danish Government in 2014 because "*they were unable to achieve their stated objective*" of investigating and prosecuting crime.[18]

Lack of detail in the draft Bill regarding the security of the data and how it will be held is a concern, particularly as cyber hacking and cyber security is a growing problem for all of us. In 2014 90% of large firms and 74% of small firms in the UK suffered a security breach.[19]

---

[16] Joint Committee on the Draft Communications Data Bill, *Final Report*, 28th November 2012, p.29: http://www.publications.parliament.uk/pa/jt201213/jtselect/jtdraftcomuni/79/79.pdf

[17] J. Shaw, *Science and Technology Committee – Oral Evidence, Investigatory Powers Bill: technology issues*, p. 9 10th November 2015: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/investigatory-powers-bill-technology-issues/oral/24378.pdf

[18] Ibid p. 2: http://itpol.dk/sites/itpol.dk/files/IPBill-Science-Tech-Committee-ITpol-submission-nov15-FINAL.pdf

[19] HM Government, *2015 Information Security Breaches Survey*, p. 6: http://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-03.pdf

The issue is not limited to the UK. The case of the US Office of Personnel Management breach which saw the often highly personal information of 21.5 million people hacked, as well as the recent hack of TalkTalk and indeed the hack conducted on the Ashley Madison site have shown that regardless of who is storing the information there are vulnerabilities.[20]

It is essential that detail about the requirements placed on the telecommunication services (who notably are given a broad definition in the draft Bill) are made clear. The public will want to know how their data will be protected. Will it be encrypted, where will it be held, will it be held in a cloud service, will it be held here in the UK or abroad, who will have access, how will they have access, what cyber protections will be put in place and should a hack, breach or attack occur who will be responsible?

Building and maintaining these systems to meet the Government's requirements may prove to be costly. The Government has quoted an estimate of £187.1m for this portion of the draft Bill. It is worth noting that estimates for similar earlier schemes were much higher. The Intercept Modernisation Scheme was projected to cost £2bn, whilst the draft Communications Data Bill came with an estimated price tag of £1.8bn.

In the latter case the estimates were attacked by industry experts who questioned where the figures had come from.

It is important that the Government properly identify where the costs incurred by their proposals will fall and that detail of what is defined in **Clause 185(1)** as an "appropriate contribution" is outlined.

Overall a great deal more clarity is needed over how this intrusive new power is intended to work, how proportionate the plan to retain 12 months of data really is, how effective it will be and what protections will be put in place to ensure the security of the data when retained. If the Government cannot conclusively prove that Internet Connection Records will be of operational use in the majority of cases, then they will be intruding on privacy for no discernible reason.

CommunicationsData

We are concerned about the definitions used to define what communications data is. The draft Bill goes to great length to provide a broad range of what is considered to be communications data and has introduced new definitions of event and entity data.

Indeed in **Sub-Clause 195(1)** we learn that "*data*" includes "*any information which is not data*." Our interpretation of this is that quite simply, anything can be defined as communications data. In a world now fueled by data this leaves little, if anything, free from potential intrusion.

Furthermore the process of authorisation for communications data is also a broad.

[20] The Atlantic, *About Those Fingerprints Stolen in the OPM Hack*, 23rd September 2015: http://www.theatlantic.com/technology/archive/2015/09/opm-hack-fingerprints/406900/

The draft Bill states throughout **Sub-Clause 46(4)** that "*any person*" can be asked for access to communications data, going so far in **Sub-Clause 46(4) (c)** as to state that "*any person whom the authorised officer believes is not in possession of the communications data but is capable of obtaining it, to obtain it and disclose it.*" This, along with **Sub-Clause 46(5) (c)** poses questions about the requirements placed on telecommunications services and their staff with regards to the data they hold and the data held by other companies.

The suggestion that the retention of "*data whether or not in existence at the time of the authorisation*" may be authorised, poses questions about necessity and proportionality and issues of pre-crime policing.

Finally we raise concern at the sheer wealth of bodies and purposes for access to communications data outlined in **Sub-Clause 46(7)**.

Bulk Powers

Of all the powers contained within the draft Bill the powers to carry out bulk interception, bulk equipment interference and the collection, retention and use of bulk personal datasets are the most intrusive for ordinary law abiding citizens. The lack of detail in the draft Bill regarding how they work in practice or how they affect members of the public is of concern, particularly as these powers have now been avowed and therefore detail of their use will be known.

We know that bulk personal datasets involve the collection and storage of the private or personal data of any and all British citizens whether dead or alive, innocent or suspect poses beyond that little detail is known, leading us to assume that any State dataset (datasets which we are all obliged without choice to appear on simply by being a British citizen) will be gathered, retained and analysed beyond the basic intended need/use of the dataset. That means birth and death records, health records and national insurance numbers to name but a few.

Should our assumption be accurate, more detail must be provided about what impact the use of these bulk personal datasets will have on the citizen including how their personal information can be intruded upon – even in the process of determining them as not being a person of interest.

The intelligence agencies have to be able to demonstrate exactly why they need these powers in bulk and what benefit bulk provides rather than the process of requesting data on a specific target in the course of an operation. To date none of this has happened.

Furthermore for the use of such data to be given the proper scrutiny and have the strongest of safeguards, the role of the Judicial Commissioner overseeing the use of the data should be strengthened.

The draft Bill proposes that the Judicial Commissioners will only have a role in reviewing the acquisition, retention use or disclosure of bulk personal datasets. It should be the case that the Commissioners are responsible for properly auditing, inspecting and investigating the use of BPDs.

It's only through proper scrutiny that the use of these powers can be justified. Of additional concern is that organisations served with a BPD warrant will not be able to query its terms.

Equipment Interference

Equipment Interference; also known as hacking or Computer Network Exploitation (CNE), has the potential to be enormously intrusive, damaging to individual devices, computer networks and systems, as well as a potential threat to the security of the internet as a whole.

The unintended consequences which can occur by the weakening of any system will enable other non-law enforcement or intelligence agency individuals to exploit the weakness, this may include malicious actors and rogue states.

In evidence to the Investigatory Powers Tribunal (IPT) **Ciaran Martin, an employee of GCHQ**, noted that Equipment interference can vary in complexity, from using the login details of a target to much more sophisticated tactics:

> "*Taking advantage of weaknesses in software. For instance a piece of software may have a "vulnerability": a shortcoming in the coding that may permit the development of an "exploit", typically a piece of software, a chunk of data, or a sequence of commands that takes advantage of the vulnerability in order to cause unintended or unanticipated behaviour to occur. This unanticipated behaviour might include allowing another piece of software – an implant called a "backdoor" or a "Trojan" – to be installed on the device.*"[21]

The lasting damage equipment interference can do to a system was highlighted by the hacking of the telecommunications firm Belgacom. The case involved three of the company's engineers being tricked into using "*spoofed*" LinkedIn and Slashdot pages which infected their machines with malware.[22] **Brian Honan, managing director of BH Consulting**, an IT consultancy firm, warned after the hack was revealed that:

> "*It would be good security practice to assume that not all instances of the malware have been identified and dealt with but rather to operate the network as if it is compromised and secure your data and communications accordingly*".[23]

[21] C. Martin, *Witness Statement in the Investigatory Powers Tribunal between Privacy International and Secretary of State for Foreign and Commonwealth Affairs and Government Communications Headquarters*, p. 6, 16th November 2015: https://privacyinternational.org/sites/default/files/CM_Witness_Statement_Signed_2015_11_16.pdf
[22] The Intercept, *Operation Socialist; The Inside Story of How Britain's Spies Hacked Belgium's Largest Telco*, 13th December 2014: https://theintercept.com/2014/12/13/belgacom-hack-gchq-inside-story/
[23] SC Magazine, *GCHQ faces new Belgacom hack allegations*, 16th December 2014: http://www.scmagazineuk.com/gchq-faces-new-belgacom-hack-allegations/article/388531/

Some forms of equipment interference can spread much further than originally intended. An example of this is the Stuxnet virus. Created by the United States and Israel it was originally targeted at Iran's nuclear enrichment facilities. As a result of the attack the virus "*escaped*" from the target system and infected the energy company Chevron's network. Chevron's general manger Mark Koelmel underlined the concern, noting "*I don't think the U.S. government even realised how far it had spread*".[24]

Given the clear risks involved, the proportionality of the tactic needs to be considered. Equipment interference should not be used as a bulk tactic designed to infiltrate broader systems, networks or organisations.

Big Brother Watch registered concern over collateral intrusion during the consultation on the Equipment Interference Code of Practice. The draft Bill and the re-published draft Code of Practice do nothing to alleviate the concern. It is unclear why someone who is not an "*intelligence target*" in their own right, as referenced in **Paragraph 2.12** of the **Equipment Interference Code of Practice**, would be targeted. This kind of loose wording could lead to potential fishing trips and middle men attacks against individuals who have not been satisfactorily linked to an investigation.

The concept of fishing trips or middle men attacks are especially important when considering the role of a 'gatekeeper' to a system, such as an IT manager or system administrator. These individuals are often completely innocent and indeed unaware about the specific information the targeted individual may hold. Specific protections must be outlined to ensure collateral damage does not occur and to ensure that the intrusion on innocent people does not take place.

In its current form **Clause 81(3)** of the draft Bill risks permitting equipment interference operations to go much further than the original target of a warrant:

> "*A targeted equipment interference warrant may also authorise the person to whom it is addressed to secure—*
>
> > *(a) the obtaining of any communications, private information or equipment data to which the purpose of the warrant relates;*
> > *(b) the obtaining of any information that does not fall within paragraph (a) but is connected with the equipment to which the warrant relates;*
> > *(c) the disclosure, in such manner as may be described in the warrant, of any material obtained under the warrant by virtue of paragraph (a) or (b).*"

Sub-Clause 81(3)(b) allows for the "*obtaining of any information*" that is "*connected*" with the equipment covered by the warrant. Given the way the internet works and the myriad of ways in which information and systems can now connect with each other this could potentially enable much broader action than was intended by the original warrant.

---

[24] Wall Street Journal, *Stuxnet Infected Chevron's IT Network*, 8th November 2014: http://blogs.wsj.com/cio/2012/11/08/stuxnet-infected-chevrons-it-network/

It should be noted that there is great contradiction between the authorisation procedures for law enforcement equipment interference warrants and those granted to the intelligence services requires clarification.

Clause 89 of the draft Bill makes it clear that when law enforcement bodies apply for a warrant to use targeted equipment interference they are not required to submit an application to the Home Secretary, only to the relevant Chief Constable, followed by review by one of the Judicial Commissioners. **Clause 84** states that when the intelligence agencies seek an equipment interference warrant they are required to seek authorisation by the relevant Secretary of State followed by review by a Judicial Commissioner.

When applying to modify a warrant the two systems are again different. Under **Clause 96** law enforcement bodies must submit any changes to a Judicial Commissioner, yet this requirement is removed for the intelligence agencies. It is unclear why as the action being authorised is the same, the only thing that has changed is the requesting body. There has been no explanation for this difference in procedure.

Encryption

Encryption is a crucial part of maintaining the security of all our online engagement, from banking to health data and beyond. Having a digital presence is now no longer a choice. We are all data citizens, were that presence to be made insecure in any way we will all be placed at risk of exposure to hacking, cyber-crime, data loss or breach. In a completely connected world this will impact access and security to the basic essentials of life.

In light of this **Clause 189** of the draft Bill which would allow the Secretary of State to "*make regulations imposing specified obligations on relevant operators*". **Sub-Clause 4(c)** allows the Secretary of State to put in place "*obligations relating to the removal of electronic protection applied by a relevant operator to any communications or data*" are a huge concern.

The importance of encryption as a tool for safeguarding the data of all citizens is recognised by a broad range of people and organisations.

For example the Information Commissioner's Office has stated that:

> "*The ICO recommends that portable and mobile devices including magnetic media, used to store and transmit personal information, the loss of which could cause damage or distress to individuals, should be protected using approved encryption software which is designed to guard against the compromise of information*."[25]

Recent headlines have shown the impact government legislation can have on the technology sector - a sector which now impacts every business whether an IT business or not and is the foundation of economic well-being of the UK.

[25] Information Commissioner's Office, *Encryption*: https://ico.org.uk/for-organisations/encryption/

Indeed should the draft Bill impose a requirement for companies to weaken or remove their encryption to comply with warrants, the UK could find itself a country which no technology company will want to engage with. Additionally the development of new technology companies wishing to start, grow or expand in the UK would be stifled. Several tech companies have already warned that this could be a threat to strong encryption in the UK.[26]

From a business perspective **The Information Technology Council**, a global umbrella group for technology firms has reacted strongly to any previous calls to weaken encryption:

"*Encryption is a security tool we rely on every day to stop criminals from draining our bank accounts, to shield our cars and airplanes from being taken over by malicious hacks, and to otherwise preserve our security and safety. We deeply appreciate law enforcement's and the national security community's work to protect us, but weakening encryption or creating backdoors to encrypted devices and data for use by the good guys would actually create vulnerabilities to be exploited by the bad guys, which would almost certainly cause serious physical and financial harm across our society and our economy. Weakening security with the aim of advancing security simply does not make sense.*"[27]

With regards to the impact weakening of encryption would have on ordinary people **Tim Cook, CEO of Apple** has highlighted that:

> "*If you halt or weaken encryption, the people that you hurt are not the folks that want to do bad things. It's the good people. The other people know where to go*"[28]

In the past Mr Cook has attacked calls from the US to undermine encryption stating that:

> "*We think this is incredibly dangerous. We've been offering encryption tools in our products for years, and we're going to stay on that path. We think it's a critical feature for our customers who want to keep their data secure. For years we've offered encryption services like iMessage and FaceTime because we believe the contents of your text messages and your video chats is none of our business.*"[29]

[26] Guardian, *Tech firms warn snooper's charter could end strong encryption in Britain*, 9th November 2015: http://www.theguardian.com/technology/2015/nov/09/tech-firms-snoopers-charter-end-strong-encryption-britain-ip-bill
[27] https://www.itic.org/news-events/news-releases/tech-responds-to-calls-to-weaken-encryption
[28] The Verge, *Tim Cook says UK plans to weaken encryption will 'hurt good people'*, 10th November 2015: http://www.theverge.com/2015/11/10/9703526/tim-cook-encryption-uk-investigatory-powers-bill
[29] TechCrunch, *Apple's Tim Cook Delivers Blistering Speech On Encryption, Privacy*, 2nd June 2015: http://techcrunch.com/2015/06/02/apples-tim-cook-delivers-blistering-speech-on-encryption-privacy/#.xkpdpk:kVGu

As far as the impact weakened encryption would have the country as a whole, including government agencies **Jon M. Peha, former Assistant Director of the White House's Office of Science and Technology Policy**, bluntly stated that:

> "*Individual computer users, large corporations, and government agencies all depend on the security features built into information technology products and services that they buy on the open market. If the security features of these widely available products and services are weak, everyone is in greater danger*".[30]

In an op-ed for the Washington Post **Mike McConnell, the former Director of the NSA, Michael Chertoff, former Secretary of Homeland Security and William Lynn, the former Deputy Secretary of Defence** argued that strong encryption was more important than government access to communications:

> "*We recognise the importance our officials attach to being able to decrypt a coded communication under a warrant or similar legal authority. But the issue that has not been addressed is the competing priorities that support the companies' resistance to building in a back door or duplicated key for decryption. We believe that the greater public good is a secure communications infrastructure protected by ubiquitous encryption at the device, server and enterprise level without building in means for government monitoring.*"[31]

Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications, is a report co-authored by the world's leading cyber-security experts, highlights the problems with the calls for scrapping or weakening encryption.

The 2015 report argues that there are three overarching problems with providing governments with "*exceptional access*".

1. Providing permanent encryption keys would diverge from the current practice of deleting keys directly after use. If a key were stolen it could compromise the entire system.
2. Allowing for this kind of access will "*substantially increase*" system complexity, with any new technology feature having to be tested by hundreds of thousands of developers around the world.
3. The security of the encryption keys is a huge problem. Creating and holding onto a key which could unlock a system would establish a weakness for if that key were to fall into the hands of an enemy it would give an attacker the ability to cause a huge amount of damage.[32]

---

[30] Jon M. Peha, *The Dangerous Policy of Weakening Security to Facilitate Surveillance*, 4th October 2013: http://users.ece.cmu.edu/~peha/Peha_on_weakened_secuirty_for_surveillance.pdf

[31] M. McConnell, M. Chertoff and W. Lynn, *Why the fear over ubiquitous data encryption is overblown*, 28th July 2015: https://www.washingtonpost.com/opinions/the-need-for-ubiquitous-data-encryption/2015/07/28/3d145952-324e-11e5-8353-1215475949f4_story.html

[32] H. Abelson, R. Anderson, S. M. Bellovin, J. Benaloh, M. Blaze, W. Diffie, J. Gilmore, M. Green, P.G. Neumann, S. Landau, R. L. Rivest, J. I. Schiller, B. Schneier, M. Specter and D.J. Weitzner, *Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications*, 6th July 2015, p. 2: http://www.crypto.com/papers/Keys_Under_Doormats_FINAL.pdf

The report poses 25 questions which the authors suggest "*must be answered in detail*" before any legislation to demand exceptional access is drafted.[33]

Put simply any part of the draft Bill which may have implications for the strength of encryption will have severe consequences for the people and the country as well. Any approach to weaken, create backdoors or simply abandon encryption must be treated with extreme caution.

Commissioner System

Big Brother Watch has called for reform to the Commissioner System on a number of occasions. The proposals for merging the three existing organisations into one body has the potential to solve many of the recurring issues, most notably:

1. The lack of funding in the current system.
2. The poor staffing of the current commissioners' offices.
3. The limited scrutiny the commissioners can provide.

The success or failure of the new scheme will rest largely with what kind of resources the Investigatory Powers Commission (IPC) is given to do its job.

Sub-Clause 176(1) notes that the Treasury will have the final say on what level of resourcing the IPC will have. This is sensible, but it is important that the process of arriving at the final figure is conducted in an open way with a broad consultation. This makes **Sub-Clause 176(2)** troubling. It stipulates that the Secretary of State must arrive at a decision on this matter based on consultation with only the Investigatory Powers Commissioner.

It would be preferable for the legislation to require consultation with a much broader range of individuals and organisations including those outside of government. The IPC will be an important part of whatever system is decided upon and this means it is vital its funding and staffing structure is properly debated. Only through this approach will citizens be assured that the intrusive powers contained within this draft Bill are overseen effectively and that the proposed system will really be an improvement.

Sub-Clause 167(1) giving the Prime Minister the power to appoint the Chief Judicial Commissioner and the Judicial Commissioners concentrates too much power in the hands of the Executive and will prevent any real independence of the Commission.

An alternative would be to allow the Judicial Appointments Commission (JAC) to make the decision on who is appointed to each position. The JAC already has a role in appointing circuit court judges, High Court judges and UK judges on the European Court of Human Rights (ECtHR). This system would give the IPC a better chance of being a properly independent body.

[33] Ibid, p. 21: http://www.crypto.com/papers/Keys_Under_Doormats_FINAL.pdf

Interception

Sub-Clause 26(2), the modification of warrants; allows for names to be added or removed, descriptions of people to change, organisations or premises to be changed, indeed any factor specified on the original warrant can be internally changed with no further review by a Judicial Commissioner.

It is important that every modification receives a high level of scrutiny; preferably with an independent Judicial Commissioner authorising not reviewing any changes. This will provide a safeguard for the citizen.

The **draft Code of Practice for interception**, published alongside the draft Bill also raises concern about the protection of the citizen. In **Paragraph 4.1** it states that

> "*Should an interception operation reach the point where individuals other than the subject of the authorisation are identified as investigative targets in their own right consideration should be given to applying for separate warrants covering those individuals.*"[34]

It should be a requirement to apply for a new interception warrant when targeting an individual who isn't the subject of the original warrant. When a new individual, previously not named by the warrant, can be proven to be of interest, it should be the case that a new warrant is sought before that individual's communications are intercepted.

Clause 42 maintains the bar on using intercepted material in court. Currently the UK is the only country that operates a common law system which entirely outlaws the use of intercept evidence in court.

Removing the bar is supported by a number of organisations and individuals including Big Brother Watch. **David Anderson QC, the Independent Reviewer of Terrorism Legislation** has stated that "*all right-minded people would like to see intercept evidence admissible in our courts*".[35]

Stuart Osborne, former Senior National Coordinator of Counter Terrorism and Head of the Counter Terrorism Command also commented that as part of a "*wide package of measures*" intercept evidence "*could be very useful in prosecution cases*."[36]

Countries which allow the use of intercept evidence include the US, Australia and New Zealand.

---

[34] Home Office, *draft Interception Code of Practice*, 4th November 2015, p. 10: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473845/6.1276_151104_INTERCEPTION_CoP_for_designer_FINAL_WEB.PDF

[35] Joint Committee on the Draft Enhanced Terrorism Prevention and Investigation Measures Bill, *Report*, 27th November 2012, p. 28: http://www.publications.parliament.uk/pa/jt201213/jtselect/jtdraftterror/70/70.pdf

[36] Ibid p. 29

Asked about the effectiveness of this **technique former Australian Commonwealth Director of Public Prosecutions, Damian Bugg QC** said: "*The use of telephone intercepts in trials for terrorism offences and other serious crimes is now quite common in Australia and I cannot understand why England has not taken the step as well.*"[37]

The effectiveness of introducing intercept evidence can be clearly seen in America. **JUSTICE** conducted a review of 10 US terror plots which involved a total of 50 individuals. With the help of intercept evidence the authorities secured both charge and conviction in each case and all within the 48 hour pre-charge detention limit. Concluding, the report argued that "*the key difference between UK and US terrorism investigation appears to [be] the extensive reliance by the police and FBI on intercept evidence in prosecuting suspected terrorists.*"[38]

The continued refusal of the Government to consider allowing intercept evidence to be used in court is made more confusing by the fact that evidence gained through equipment interference is permitted. The argument that the evidence from intercepting communications would reveal too much about the methods and work of the intelligence agencies seems nonsensical when it is permitted in a power which only recently has been avowed. Further information on why it is not possible to utilise this evidence in court would be instructive.

The draft Code of Practice for interception adds more questions. **Paragraphs 8.6 to 8.10** of the Code allow intercepted material to be disclosed to a prosecutor to help him or her "*determine what is required of him or her by his or her* duty to *secure the fairness of the proceedings*".[39] There is little information about how a disclosure of this kind would help increase the fairness of a trial. Similar passages allow for the release of information to a judge.

This is especially prescient given the fact that **Paragraph 8.14** concludes that "*nothing in these provisions allows the intercepted material, or the fact of the interception, to be disclosed to the defence*."[40] The document should at the very least outline the circumstances which could lead to a disclosure and the reasons why materials can be released to a judge and a prosecutor but not those acting for the defence.

Redress/User Notification

The draft Bill barely touches the issue of redress. **Clause 180**, which would allow an appeal to be brought in a UK court as opposed to the European Court of Human Rights (ECtHR), is a small step in the right direction. However questions about how it will work in practice need to be answered.

---

[37] D. Raab, *Fight Terror, Defend Freedom*, September 2010, p. 39: http://www.bigbrotherwatch.org.uk/files/dominicraabbookfinal.pdf
[38] 6 JUSTICE, *From Arrest to Charge in 48 Hour: L Complex terrorism cases in the US since 9/11*, November 2007: http://www.justice.org.uk/data/files/resources/37/From-Arrest-to-Charge-in-48-Hours-1-November-2007.pdf
[39] Home Office, *Draft Code of Practice for the Interception of Communications*, 4th November 2015, p. 32: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/401866/Draft_Interception_of_Communications_Code_of_Practice.pdf
[40] Ibid, p. 33

Sub-Clause 180(1) notes that appeals may be brought on a "*point of law*". This implies that appeals may only be brought on the Tribunal's interpretation of legal principles. Clarity must be provided on whether or not appeals can be made for errors of fact or procedural unfairness as well. If this is not the case an explaniation should be provided as to why the Government rationale for limiting the grounds for appeal.

Sub Clause 180(4) also raises issues:

> "*The Tribunal or court must not grant leave to appeal unless it considers that—*
>
> *(a) the appeal would raise an important point of principle or practice, or*
>
> *(b) there is another compelling reason for granting leave.*"

It is unclear whether this could be used to further limit the instances under which someone could appeal a decision by the Investigatory Powers Tribunal (IPT).

Sub clause 171(1) makes clear that the IPT must inform a person of any error relating to that person, however **Sub-clause 171(2)** requires clarification. It states that before any report is made, both the IPT and the IPC must agree that an error has taken place and that disclosure would be in the public interest. More information is needed about how decisions will be arrived at and in particular how the public interest test will be applied.

A proper system of redress is vital to ensuring that the citizens can be confident that these powers are being used in their best interests. The draft Bill currently fails to do that.

Big Brother Watch have called for reform in this area for a number of years. Any workable system must begin with some form of user notification. Germany, Belgium and from 2016 the State of California will all use a system of user notification so it isn't a new or indeed unique proposal.

Innocent individuals are informed that they have been the target of surveillance once the case has been closed.

If the same process were adopted in the UK it would increase the amount of transparency as well as provide an opportunity for redress - allowing the individual to clear their name. Previously we have stated that notification should take place 12 months after the conclusion of an investigation. Under the proposals there would also be the opportunity to apply to a judge to extend this period in 6 monthly increments.[41]

Fundamental change to the way the Investigatory Powers Tribunal functions is necessary and is lacking from the draft Bill.

[41] Big Brother Watch, *Off the Record: How the police use surveillance powers*, October 2014, p. 8: http://www.bigbrotherwatch.org.uk/wp-content/uploads/2014/10/Off-the-Record-BBW-Report1.pdf

The Royal United Services Institute's (RUSI) *Democratic Licence to Operate* contains a number of recommendations which would help the IPT "*make its business less opaque to the public*".[42] At present the IPT is far too secretive. At the very least it should adopt RUSI's recommendation of holding open hearings.[43] This would help increase public confidence in its work and in the process increase awareness of the work the Tribunal does. It should be noted that this would not preclude the Tribunal from holding secret proceedings when it could be demonstrated that there was a pressing need to do so.

Terminology

Finally, it should be noted that throughout the draft Bill terms are often very loose or broadly described. For surveillance legislation to be meaningful and for the general public to be reassured and have a comprehensive understanding of what terms mean, how techniques and powers can be used and who will have access to or hold their data, the Bill should look to offer further clarity. This is not to divulge the secrets of the operation but to be precise rather than vague.

[42] Royal United Services Institute*, A Democratic Licence to Operate*, 13th July 2015, p. 113: https://rusi.org/sites/default/files/20150714_whr_2-15_a_democratic_licence_to_operate.pdf
[43] Ibid p. 113