BIG BROTHER WATCH
DEFENDING CIVIL LIBERTIES, PROTECTING PRIVACY

Science and Technology Select Committee - Technology aspects of the Draft Investigatory Powers Bill

November 2015

About Big Brother Watch

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

Specific to this inquiry we have campaigned against the draft Communications Data Bill and the Data Retention and Investigatory Powers Act 2014. We have also produced reports on subjects such as Police access to Communications Data and the use of RIPA by local councils.

Key Points

- **More clarity is needed over how the ICRs of individuals will be kept secure.**
- **The clauses on Equipment Interference risk opening ordinary people to surveillance.**
- **Encryption is a necessary tool for citizens and must be protected.**

This response will focus on the third point raised by the Committee’s call for evidence. It will consider the consequences the Bill may have for citizens and their use of IT.

Response

Interception

The proportionality of any form of interception is an issue Big Brother Watch has raised repeatedly in the past. We have stressed that interception should be targeted on people suspected of participating in illegal activity rather than a broad sweep of interception used as a way of finding potential leads.

The draft Bill proposes two forms of interception; targeted and bulk. Whilst we acknowledge that the draft Bill has attempted to outline safeguards to protect the data of innocent people from being intercepted we feel that there remains weakness in the proposed system.

The process of only requiring Judicial Commissioners to “review” the warrants already authorised by a Secretary of State does not provide the “double lock” the Home Secretary indicated on presentation of the draft Bill. We would prefer to see full independent judicial authorisation, not the proposed process of “review”.

We are also concerned by the proposals in Clause 26 of the draft Bill; the modification of warrants, these proposals allow an authorised warrant to be fundamentally modified. Meaning that names can be added or removed, descriptions of people, organisations or premises can be changed, indeed any factor specified on the original warrant can be internally changed, with no further review by a Judicial Commissioner. This needs to be reviewed so any modification is given a high level of scrutiny and authorisation; preferably by an independent Judicial Commissioner authorising not reviewing, to ensure that external scrutiny of a warrant is permitted. This will provide a safeguard for the citizen that warrants are not changed on a whim and signed off internally.

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.”*[1]

It should be a requirement to apply for a new interception warrant when targeting an individual that 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.

[1] Home Office, *draft Interception Code of Practice*, p. 10, November 2015:

Equipment Interference

The capability of Equipment Interference; also known as Computer Network Exploitation (CNE) or hacking, has the potential to be very damaging to individual devices, computer networks and systems as a whole.

The unintended consequences which can occur during Equipment Interference are a very real threat. Put simply, weakening a system does not mean that only law enforcement or the intelligence agencies can exploit it. The system can be exploited by anyone who uncovers the weakness, including malicious actors, rogue states or non-Government hackers.

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.[2] Brian Honan, managing director of BH Consulting, an IT consultancy firm, warned after the hack was revealed that:

> "*It would be good security practise 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*".[3]

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*".[4]

Given the risks involved the proportionality of the tactic needs to be considered. If Equipment Interference is to be used at all it should only be deployed on individuals who are of genuine interest to law enforcement or the intelligence agencies, rather than as a bulk tactic designed to infiltrate broader systems, networks or organisations which may engage with innocent members of society.

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 and unexplained wording could lead to potential fishing trips against individuals who haven't been satisfactorily linked to an investigation.

[2] 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/

[3] SC Magazine, *GCHQ faces new Belgacom hack allegations*, 16th December 2014: http://www.scmagazineuk.com/gchq-faces-new-belgacom-hack-allegations/article/388531/

[4] 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/

This is 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 a 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.

The concern about the process extending beyond the target is present in the draft Bill, sub-clause 81(3):

> "*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-section (b) allows 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.

The contradictory authorisation procedures for the two forms of Equipment Interference warrants also raise concern.

With regards to the warrantry process 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. Once internal sign off has been sought the request is then reviewed by one of the Judicial Commissioners. The intelligence agencies when seeking a warrant to conduct bulk equipment interference however are required to seek authorisation by the relevant Secretary of State and then the authorised warrant is reviewed by a Judicial Commissioner.

When applying to modify a warrant the two systems are again different. Whilst law enforcement bodies must submit any changes to a Judicial Commissioner this requirement is removed for the intelligence agencies, that the intelligence agencies work in bulk which poses a threat to the security of all citizens not just targets, further authorisation of the changes should be sought.

There has been no explanation for this difference in procedure.

Internet Connection Records (ICRs)

ICRs have been characterised as the online equivalent of a phone bill. Dr Paul Bernal, a lecturer in IT law, has raised concerns about the amount of information that would need to be stored:

> "*We do almost everything online. We bank online. We shop online. We research online. We find relationships online. We listen to music and watch TV and movies online. We plan our holidays online.*"[5]

Analysing our internet history or what sites we have visited can provide a rich source to identify our likes, dislikes, potential religion or even whether or not a person may be suffering from a health condition. It has also been noted by Dr Bernal unlike a phone bill we don't just talk online.

Concerns have been raised about how feasible it will be to separate the content of a message from the ICR. Giving evidence to the Science and Technology Select Committee John Shaw noted that in reality the line between the two was "*incredibly blurred*".[6]

In the same session Matthew Hare, CEO of Gigaclear, also noted the potential issue:

> "*For some things it is very clear. If you are watching a movie on Netflix, receiving that movie is clearly content. If you happened to be resizing your screen you might be passing code back to Netflix about something you wanted to pass across the internet, because every time you resize your screen it sends control information back to Netflix.*"[7]

If the Government want this new power they have to explain how they intend to safeguard the privacy of citizens first and be 100% clear how they propose the technology will work.

This is not the first time retention of this data has been proposed. The draft Communications Data Bill proposed the retention of weblogs. The Joint Committee convened to scrutinise 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*"[8].

[5] P. Bernal, *A few words on 'Internet Connection Records'*, 5th November 2015: https://paulbernal.wordpress.com/2015/11/05/a-few-words-on-internet-connection-records/

[6] 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

[7] M. Hare, *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

[8] 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 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.*"[9]

It is important that clear guidelines are presented to the telecommunication services regarding the protection and security of the data. The draft Bill is not at all clear or indeed explicit on what will be required.

A survey, conducted earlier this year for the UK Government, by PricewaterhouseCoopers found that in 2014 90% of large firms and 74% of small firms in the UK had suffered a security breach. Additionally 59% of those surveyed expected the number of breaches to rise in the following year.[10] Clearly there is a problem with data protection and so far there has been no explanation from the Government over how they propose the companies are to keep the information of their customers safe.

Cases such as the US Office of Personnel Management breach, which saw the often highly personal information of 21.5 million people hacked, not to mention the recent hack of Talk Talk and indeed the hack conducted on the Ashley Madison site have shown that regardless of who is storing the information there are vulnerabilities.[11]

This threat to the data has been noted by John Shaw, Vice President, Project Management at Sophos, in evidence to the Science and Technology Committee:

> "*It is not just the cost of the data; the exposure of everyone in the UK's data to people trying to hack it to do bad things with it is a very meaningful difference.*"[12]

The concern is echoed by Matthew Hare in his evidence:

> "*All you will do is create a massive database of who uses the internet for what and when, to be stored across a whole range of different service providers to make sure you have the content available, and I would question whether keeping that secure and safe is always going to be the case.*"[13]

[9] 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

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

[11] 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/

[12] 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

[13] M. Hare, *Science and Technology Committee – Oral Evidence, Investigatory Powers Bill: technology issues*, p. 2: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/investigatory-powers-bill-technology-issues/oral/24378.pdf

Bulk Collection

The draft Bill contains provisions for Bulk Interception, Bulk Equipment Interference and Bulk Personal Datasets. At present there is limited information about how these powers work in practice or indeed how they affect citizens. What we do know is that bulk personal datasets involve the collection and storage of the private or personal data of all British citizens whether dead or alive, innocent or suspect.

More detail must be provided about how the privacy of innocent people is impacted, as well as how their personal information can be intruded upon. Additionally 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.

Encryption

Section 189 of the draft Bill will threaten the security of citizens as well as the security of business and the country as a whole. The section would allow the Secretary of State to "*make regulations imposing specified obligations on relevant operators*". Specifically sub-section 4(c) allows the Secretary of State to impose "*obligations relating to the removal of electronic protection applied by a relevant operator to any communications or data*".

Several tech companies have warned that this could be a threat to strong encryption in the UK.[14] The importance of encryption as a tool for safeguarding the data of all citizens is something which has been recognised by the Information Commissioner's Office:

> "*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*."[15]

In a post in March 2014 Mark Zuckerberg the CEO of Facebook, warned that "*To keep the internet strong, we need to keep it secure*". Encryption he said was a vital tool in this effort:

> "*The internet works because most people and companies do the same. We work together to create this secure environment and make our shared space even better for the world*."[16]

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 everyday 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.*"[17]

Encryption is a vital tool in a world dominated by technology and data. As an example of the importance of encryption, without strong encryption there would almost certainly be little or no trust in online banking.

[14] 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

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

[16] M. Zuckerberg, *Facebook Post*, 13th March 2014: https://www.facebook.com/zuck/posts/10101301165605491

[17] https://www.itic.org/news-events/news-releases/tech-responds-to-calls-to-weaken-encryption

Tim Cook the CEO of Apple CEO highlighted the affect weakening of encryption would have on ordinary people:

> "*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*"[18]

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

> "*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.*"[19]

Jon M. Peha, former Assistant Director of the White House's Office of Science and Technology Policy, put it more bluntly:

> "*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*".[20]

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 that 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.*"[21]

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, which highlights the problems with the calls for scrapping or weakening encryption.

[18] 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

[19] 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

[20] 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

[21] 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

The report is similar to one written twenty years ago when calls to regulate the internet by building in backdoors, or creating keys to provide "exceptional access" into systems were being debated in the USA.

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.[22]

The report poses 25 questions which the authors suggest "*must be answered in detail*" before any legislation to demand exceptional access is drafted.[23]

The words of Admiral James A. Winnefield, Vice Chairman of the Joint Chiefs of Staff should also be noted:

> "*But I think we would all win if our networks are more secure. And I think I would rather live on the side of secure networks and a harder problem for Mike [NSA Director Mike Rogers] on the intelligence side than very vulnerable networks and an easy problem for Mike and part of that, it's not only is the right thing to do, but part of that goes to the fact that we are more vulnerable than any other country in the world, on our dependence on cyber. I'm also very confident that Mike has some very clever people working for him, who might actually still be able to get some good work done.*"[24]

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.

[22] 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

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

[24] Ibid, p. 10: http://www.crypto.com/papers/Keys_Under_Doormats_FINAL.pdf