BIG BROTHER WATCH
DEFENDING CIVIL LIBERTIES, PROTECTING PRIVACY

Joint Committee on Human Rights – Written Evidence on the Draft Investigatory Powers Bill

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 oversight and authorisation systems need more scrutiny to ensure they will protect citizens.**
- **Clauses on bulk powers, Equipment Interference and Interception risk permitting the surveillance of innocent citizens.**
- **Encryption must be protected.**

Response

At 296 pages long the draft Investigatory Powers Bill is a long and complex document which proposes a broad range of intrusive powers including a number of bulk powers which have the potential to impact on the human rights of all citizens. Should this draft Bill become law, proper independent safeguards will be necessary.

It should be noted that the Joint Committee tasked with scrutinising the draft Bill have only been given 7 weeks to conduct their evidence gathering and report to Parliament. Compared with previous scrutiny committee's this is not enough time to fully assess the impact the proposals will have on citizens.

Internet Connection Records

The Government must show exactly how these proposals will make citizens safer and how they are technically feasible. The intrusiveness of this newly proposed power has been recognised by both technologists and legal experts.[1] [2] In an age where severe hacks such as TalkTalk and Ashley

Madison can occur it is more important than ever that proper safeguards are mandated before any retention takes place. So far there has been no detail of how the information will be kept secure.

It should be noted that Denmark previously implemented a data retention scheme similar to the proposed system. In 2014 the Danish government repealed the measures because "*they were unable to achieve their stated objective*" of investigating and prosecuting crime.[3]

Bulk Powers

The powers to carry out bulk interception, bulk equipment interference and collect and analyse bulk personal datasets all have the potential to be very intrusive to citizens. The information about how these powers work in practice or indeed clear information about how they affect members of the public is clearly lacking.

All we know is 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.

The extent to which the privacy of citizens will be intruded upon must be properly explained. Without clarity on the issue of bulk personal datasets in particular it is impossible to properly scrutinise the proposal.

Equipment Interference

This capability has the potential to be very damaging to the privacy of all citizens. A number of clauses require further scrutiny because in their current format they risk subjecting citizens to unnecessary surveillance.

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

---

[1] A. Kennard, Written Evidence regarding the Investigatory Powers Bill, p. 1, 25th November 2015: http://www.me.uk/IPBill-evidence1.pdf

[2] IT-Political Association of Denmark, *Written evidence to the Science and Technology Committee -Investigatory Powers Bill: Technology Issues*, p. 4: http://itpol.dk/sites/itpol.dk/files/IPBill-Science-Tech-Committee-ITpol-submission-nov15-FINAL.pdf

[3] IT-Political Association of Denmark, *Written evidence to the Science and Technology Committee -Investigatory Powers Bill: Technology Issues* p. 2: http://itpol.dk/sites/itpol.dk/files/IPBill-Science-Tech-Committee-ITpol-submission-nov15-FINAL.pdf

Clauses 89 and 84 present two different authorisation schemes: one for law enforcement and the other for the intelligence agencies. The intelligence agencies must seek approval from both a secretary of state and a Judicial Commissioner. No Secretary of State is involved in the authorisation of law enforcement warrants. The differing levels of scrutiny have not been explained.

Clause 96 introduces another unexplained difference. Whilst modifications to law enforcement warrants are subjected to judicial scrutiny this requirement does not apply to the intelligence agencies. Again it is unclear why this is the case. The action being authorised is the same, the only thing that has changed is the requesting body.

Encryption

Encryption is a basic protection for citizens in the modern age, however **Sub-Clause 189(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*".

A number of technology companies have warned that this could be a threat to strong encryption in the UK. Encryption protects ordinary citizens and is vital to a myriad of online activities. Its use has been supported by the ICO[4], Mark Zuckerberg[5], the Information Technology Industry Council[6] and Tim Cook.[7] Any clauses that seem like they may weaken it will also harm innocent citizens and must therefore be fully scrutinised and if necessary removed from the final Bill.

Interception

The clauses on interception have the potential to allow the surveillance of innocent people. **Clause 26** allows an authorised warrant to be fundamentally modified. Under **Sub-Clause 26(2)** 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 changed, with no further review by a Judicial Commissioner. It is important that every modification receives a high level of scrutiny; under these proposals this will not happen.

Judicial Authorisation

Despite assurances of a "double lock" the authorisation procedure outlined in the draft Bill does not amount to judicial authorisation. 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".*

---

[4] Information Commissioner's Office, *Encryption*: https://ico.org.uk/for-organisations/encryption/
[5] M. Zuckerberg, *Facebook Post*, 13th March 2014: https://www.facebook.com/zuck/posts/10101301165605491
[6] Information Technology Industry Council, *Tech Responds to Calls to Weaken Encryption*, 19th November 2015: https://www.itic.org/news-events/news-releases/tech-responds-to-calls-to-weaken-encryption
[7] 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

A system which allows for the Secretary of State to authorise a warrant and then for a Judicial Commissioner to review the decision already made, fails to address any of the current systems concerns. The new proposals provide little assurance that a decision is being made independently and leaves the UK at odds with the other Five Eye countries.

It is simply not sustainable to allow a Secretary of State to play a leading role in authorising warrants. In 2014 alone the Home Secretary signed off 2,345 interception warrants, equivalent to 6 every day.[8] **Martin Chamberlain QC** notes 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*".[9]

The Commissioner System

If the human rights of UK citizens are to be protected it is vital that there is an effective system of oversight. The proposals in the draft Bill have the potential to fix some of the issues the current system has. However, much will depend on what level of resourcing and staffing the body receives. The creation of this system should be a matter of debate. It is of concern to see that **Sub-Clause 176(2)** 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.

The independence of the Investigatory Powers Commission should also be scrutinised. **Sub-Clause 167(1)** states that the Prime Minister is to appoint both the Chief Judicial Commissioner and the Judicial Commissioner. If the IPC is to be seen as properly independent the responsibility of appointing those in it should fall to a body such as the Judicial Appointments Commission (JAC). Without proper independence the IPC will be unable to ensure the powers contained within this draft Bill will be used in the best interest of citizens.

Redress/User Notification

Whilst **Clause 180,** which allows an appeal to be brought in a UK court as opposed to the ECtHR, is a good step, the issue of redress, vital to protecting citizens, barely features in the draft Bill. **Sub-Clause 180(1)** notes that appeals may be brought on a "*point of law*". Further clarification is needed over whether or not this is the only basis for an appeal.

[8] 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
[9] 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

A proper system of user notification is vital to ensuring that the citizens can be confident that these powers are being used in their best interests. It is something that the draft Bill currently fails to provide. Far from being an untested idea Germany, Belgium and from January 2016 the State of California will all use a system of user notification. In the past Big Brother Watch has stated that notification should take place 12 months after the conclusion of an investigation with opportunity for application to a judge to extend this period in 6 monthly increments.[10]

[10] 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