Written Evidence to the Joint Committee on the Draft Investigatory Powers Bill Submitted by Human Rights Watch

December 21, 2015

Introduction and Summary

1. Human Rights Watch welcomes the opportunity to provide comments on the draft UK Investigatory Powers Bill (IP Bill). Human Rights Watch is an international nongovernmental organization that monitors and reports on human rights in about 90 countries around the world. We have documented the harms of overbroad and unchecked surveillance for the work of journalists, lawyers, and civil society organizations and advocated for stronger protections for the right to privacy in the digital age in the UK, US, and globally.

2. The Internet has become central to nearly every aspect of our lives and is the cornerstone of today's modern global economy. It has also helped advance global human rights, enabling independent civil society and individuals to advocate for their rights and demand accountability from their governments. At the same time, we also now live in an age of "big data," when our communications and activities routinely leave rich digital traces that can be collected, analyzed, and stored at low cost. In parallel, commercial imperatives drive a range of companies to amass vast stores of information about our social networks, health, finances, and shopping habits.

3. These trends have led to what many have deemed the "golden age of surveillance," where law enforcement and security agencies have access to an unprecedented amount of investigatory material enabled by the digital world, including entirely new forms such as location data or web browsing histories.[1] Declining costs of computing and data storage have also removed many financial or practical constraints to conducting surveillance or data collection.

[1] Peter Swire, "'Going Dark' Versus a 'Golden Age for Surveillance,'" Center for Democracy & Technology, November 28, 2011, https://cdt.org/blog/%E2%80%98going-dark%E2%80%99-versus-a-%E2%80%98golden-age-for-surveillance%E2%80%99/ (accessed December 21, 2015); Peter Swire, Testimony at US Senate Judiciary Committee Hearing, "Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy," July 8, 2015, http://www.judiciary.senate.gov/imo/media/doc/07-08-15%20Swire%20Testimony.pdf (accessed December 21, 2015).

4. Unfortunately, corresponding legal protections for the right to privacy have not kept pace with technological change. The UK Government's Regulation of Investigatory Powers Act of 2000 was passed years before the advent of modern social media or widely available smart phones. New digital investigatory techniques like equipment interference/computer network exploitation (CNE) were not even contemplated by many policymakers 15 years ago.

5. Human Rights Watch believes the UK's surveillance legislation should be overhauled so that a broad range of investigatory powers are subject to the rule of law and adequate oversight and supervision, and to ensure privacy is protected. However, the draft IP Bill introduced on November 4, 2015 falls gravely short in preventing unjustified or disproportionate breaches of privacy and other rights and in providing transparency, adequate oversight, or access to effective remedies. Many of the provisions are vaguely and broadly drawn, leaving the public unsure of the scope and scale of measures it enables or how privacy will be affected by those measures. In its current form, the bill would legitimize mass surveillance and extraterritorial warrants served on companies outside the UK for surveillance and device hacking, which sets a worrying precedent that could jeopardize the rights of UK citizens and that other governments, including abusive regimes, might follow.

6. Human Rights Watch urges the joint committee to incorporate the following in its recommendations to Parliament:
    a. ***Require meaningful judicial authorization:*** Independent, prior judicial authorization should be required for all powers authorized under this act and judges should be empowered to review the merits of the warrant application and make an independent determination of its legality, necessity, and proportionality.
    b. ***Bulk Data Collection and Interception are Fundamentally Disproportionate:*** Authorities should be required to demonstrate to an independent judicial authority that the measures sought are the least intrusive means for achieving the defined goal, that more tailored means have been exhausted, and that the bulk measures would be effective at achieving the defined goal. The larger and more indiscriminate the measure of collection, the more difficult this standard will be to meet, foreclosing bulk collection as a routine or standard measure.
    c. ***Refrain from Undermining Encryption and Digital Security:*** Strong encryption and analogous measures are essential to both privacy and security online. Requirements that telecommunications or Internet companies "maintain technical capabilities" are not sufficiently defined in the bill to ensure they do not disproportionately harm rights. The bill should be amended to ensure authorities are prohibited from imposing obligations on

Internet service providers to weaken security measures or design their systems to incorporate measures for exceptional access into encryption by UK authorities.

d. ***Equipment Interference Powers Require More Scrutiny:*** Equipment interference powers raise novel technical and legal issues that deserve greater scrutiny before the bill moves forward. Given the potentially broader harm to cybersecurity, Human Rights Watch questions the proportionality and necessity of equipment interference as a whole, and these concerns are more acute for bulk equipment interference. The committee should seek greater public transparency from intelligence and law enforcement agencies into how equivalent provisions have been applied under current law, and how this might change under the IP Bill. The bill should also be amended to more narrowly define the information and equipment that can be targeted under targeted equipment interference warrants.
e. ***Extraterritorial Impact:*** The bill should be amended to forbid authorities from serving warrants on service providers outside the UK. Otherwise, the bill in its current form could set a deeply troubling global precedent. Other governments could demand of companies similar access, potentially including requests for data of UK citizens by authoritarian governments abroad.
f. ***Remedy Remains Ineffective:*** The draft bill falls short in providing adequate transparency and removing the significant barriers to redress that exist in the current system. The bill should require notification to individuals whose communications have been intercepted or whose data has been collected, though notice could be delayed under specified circumstances. The Investigatory Powers Commissioner and other oversight bodies should be required to inform individuals when it is determined that their rights have been breached so they can seek recourse.

The Right to Privacy in the Digital Age

7. Digital technologies have enabled surveillance on an unprecedented scope and scale. A landmark 2014 report by the UN High Commissioner for Human Rights examined the regulation of surveillance powers globally and found that many governments have failed to meet their obligations to protect privacy under international human rights standards. The High Commissioner found practices in many states revealed “a lack of adequate national legislation and/or enforcement, weak procedural safeguards, and ineffective oversight.”[2] Combined with a “disturbing lack of governmental transparency,” these failings have “contributed to a lack of

[2] UN Human Rights Council, Report of the Office of the United Nations High Commissioner for Human Rights, “The Right to Privacy in the Digital Age,” U.N. Doc. A/HRC/27/37, June 30, 2014, http://www.ohchr.org/Documents/Issues/DigitalAge/A-HRC-27-37_en.doc (accessed December 12, 2015).

accountability for arbitrary or unlawful interference in the right to privacy." Accordingly, the High Commissioner provided guidance for states to ensure surveillance is conducted consistent with human rights requirements:

a. ***Mass surveillance is by nature indiscriminate, arbitrary, and disproportionate.*** Large-scale collection practices often fall afoul of the requirement of proportionality. Proportionality requires that the government use the least intrusive means to achieve a legitimate aim and the onus is on the government to show that it has complied with that requirement.
b. ***Communications data is often just as sensitive*** and revealing as the content of communications and merits stronger protection than many national laws currently grant. This was implicitly recognized by the Court of Justice of the European Union (CJEU) in *Digital Rights Ireland* when it invalidated the EU's Data Retention Directive, noting that the blanket nature of data retention mandates flouts the principle of proportionality.[3] The UN High Commissioner for Human Rights also noted that "Even the mere possibility of communications information being captured creates an interference with privacy, with a potential chilling effect on rights, including those to free expression and association. The very existence of a mass surveillance programme thus creates an interference with privacy. The onus would be on the State to demonstrate that such interference is neither arbitrary nor unlawful."[4]
c. The High Commissioner found that mandatory third-party data retention requirements, where the government requires Internet or mobile service providers to store data about all customers that the government can later access, "***appear neither necessary nor proportionate***" since they interfere with the privacy of all users, regardless of whether they are under suspicion of wrongdoing.
d. States should also ensure ***effective oversight to safeguard against abuse, as well as remedy*** for violations of rights linked to digital surveillance. Prior, independent judicial authorization is best practice in this regard, along with oversight from all branches of government.

---

[3] *Digital Rights Ireland Ltd. v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, Judgement, April 8, 2014, Joined Cases C-293/12 and C-594/12, ECLI:EU:C:2014:238, http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&text=&pageIndex=0&part=1&mode=lst&docid=150642&occ=first&dir=&cid=314051 (accessed December 21, 2015); Cynthia Wong, "Dispatches: Victory for Digital Privacy on Data Retention," Human Rights Watch, April 9, 2014, https://www.hrw.org/news/2014/04/09/dispatches-victory-digital-privacy-data-retention.
[3] UN Human Rights Council, Report of the Office of the United Nations High Commissioner for Human Rights, "The Right to Privacy in the Digital Age," U.N. Doc. A/HRC/27/37, June 30, 2014, para 20.
[4] Ibid.

8. In July 2015, the UN Human Rights Committee reiterated many of these conclusions in its review of the UK's implementation of the Article 17 right to privacy under the International Covenant on Civil and Political Rights (ICCPR). The Committee expressed concern that the UK's laws "allows for mass interception of communications and lacks sufficient safeguards against arbitrary interference with the right to privacy" and provided weaker safeguards for interception of so-called "external communications" sent or received outside the UK. The Committee called on the UK government to do the following:[5]
    a. Ensure surveillance and data collection practices comply with the ***principles of legality, proportionality, and necessity, regardless of the nationality or location of the individuals*** whose communications are under surveillance.
    b. Ensure ***robust oversight systems over surveillance, interception, and intelligence sharing*** are in place, including by providing for "***judicial involvement in the authorization of such measures in all cases"*** and strong and independent oversight mandates to prevent abuse.
    c. Ensure access to communications data is limited to the extent ***strictly necessary for prosecution of the most serious crimes*** and is dependent upon ***prior judicial authorization.***
    d. Ensure ***access to effective remedies*** to address cases of abuse.

9. The current draft of the Investigatory Powers Bill falls fatally short of these requirements and should be revised considerably. We highlight several issues of particular concern below and urge the Joint Committee to raise these concerns in its report on the bill and directly with the government.

Require Meaningful Judicial Authorization

10. In introducing the IP Bill on November 4, 2015, Home Secretary Theresa May stated it would create a "world-leading oversight regime," requiring a "double-lock" of executive and judicial approval.[6] However, while the bill is an improvement over the current framework, the bill's authorization mechanisms do not hold up under scrutiny and are inadequate to safeguard against arbitrary and unlawful intrusions on privacy.

---

[5] UN Human Rights Committee, "Concluding observations on the seventh periodic report of the United Kingdom of Great Britain and Northern Ireland," U.N. Doc. CCPR/C/GBR/CO/7, August 17, 2015, http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G15/182/29/PDF/G1518229.pdf?OpenElement (accessed December 21, 2015).
[6] Theresa May, Oral statement to Parliament, "Home Secretary: Publication of draft Investigatory Powers Bill," November 4, 2015, https://www.gov.uk/government/speeches/home-secretary-publication-of-draft-investigatory-powers-bill (accessed December 21, 2015).

11. The bill provides only a limited role for judicial commissioners in approving warrants for various investigatory powers throughout the bill, applying "the same principles as would be applied by a court on an application for judicial review." Thus, the judges would only be able to assess whether the authorities followed the correct procedure and acted reasonably and within their powers. The bill does not contemplate independent, substantive judicial review of executive decisions, nor of the evidence presented by authorities that supports them. In all, this structure is inadequate to ensure effective supervision of the government's broad surveillance powers.

12. Some intrusive and potentially broad surveillance powers would not require approval by judicial commissioners. Specifically, under the bill, there is no judicial role in approving "targeted" requests to access communications data and warrants issued to companies to retain data. Given the growing recognition of the sensitivity of communications data, this omission is troubling. Similarly, judges play no role in approving broadly defined national security or technical capability notices served on telecommunications operators.[7] These notices are ill-defined and enable exceptionally broad powers. National security notices can require service providers to "carry out any conduct … for the purpose of facilitating anything done by an intelligence service under any enactment other than this Act," if in the interest of national security. Technical capability notices can impose obligations on service providers to "provide facilities or services" or "the removal of electronic protection" to any communications or data. These broadly and ill-defined powers raise novel legal and technical questions that should be subject to substantive as well as procedural prior review by an independent judge, along with scrutiny by other oversight bodies.

13. Authorities would also be able to proceed without even this pro forma judicial approval temporarily if they deem it "urgent," though they would need to seek approval after the fact. Whether a case is "urgent" would be decided by the person who issued the warrant, and such cases would not be limited to situations involving imminent threats to life or property. "Urgency" should be conservatively defined in the law, and the government denied the use of such collected data, as well as the use of evidence derived from such data, if on subsequent review a court determines that the initial determination of urgency was an abuse of executive discretion.

14. ***Recommendations***:
    a. Judicial commissioners should be empowered to review evidence presented in support of a warrant and make an independent determination of the warrant's legality, necessity, and proportionality.

[7] IP Bill, Clauses 188, 189

b. Independent judicial authorization should be required for all powers authorized under the act, including targeted access to communications data, data retention warrants, and national security and technical capability notices.
c. Judges should have access to external technical expertise, with security clearance if necessary, in assessing the necessity and proportionality of proposed powers and warrants.

Bulk Data Collection and Interception Fundamentally Disproportionate

15. The bill provides an explicit legal basis for interception and communications data collection (including that of UK citizens) in bulk, putting longstanding practices on clear legal footing.[8] While bringing current practices within the rule of law is desirable, mass or large-scale surveillance is fundamentally arbitrary and disproportionate.

16. The right to privacy is implicated when personal data or communications are collected—in the most commonly understood use of the word—and can be violated if such collection is arbitrary, unlawful, or indiscriminate. This is true regardless of whether the information is subsequently processed, examined, or used by the government.

17. Dragnet searches or collection on large groups without some threshold showing of necessity and proportionality should be presumptively impermissible. In the US, one bulk communications data program was halted after two independent oversight bodies with access to classified information found that the program was not essential to preventing terrorist attacks.[9] This program violated the privacy of potentially millions of individuals, while providing no unique intelligence value. It would have continued to do so had the program not come to light and been subjected to independent scrutiny.

18. ***Recommendation***:
    a. Authorities should be required to demonstrate to an independent judicial authority that the measures sought are the least intrusive means for achieving the defined goal, that more tailored means have been exhausted, and that the bulk measures would be effective

[8] The term "bulk" is not sufficiently defined in the draft bill or existing legal frameworks. For purposes of this submission, we assume that this term could apply to a range of large-scale interception or data collection programs, including mass interception of all Internet traffic flowing through trans-Atlantic fiber optic cables, potentially nationwide collection of communications data, or other large scale programs that do not premise collection on the prior identification of a specific individual or group.
[9] Peter Swire, "The USA FREEDOM Act, the President's Review Group and the Biggest Intelligence Reform in 40 Years," Privacy Perspectives Blog, June 8, 2015, https://iapp.org/news/a/the-usa-freedom-act-the-presidents-review-group-and-the-biggest-intelligence-reform-in-40-years (accessed December 21, 2015).

at achieving the defined goal. The larger and more indiscriminate the measure of collection, the more difficult this standard will be to meet, foreclosing bulk collection as a routine or standard measure.

Refrain from Undermining Encryption and Security

19. The Home Secretary has stated that the bill "will not ban encryption or do anything to undermine the security of people's data."[10] However, in addition to imposing general duties to give effect to warrants, the bill would allow authorities to require private telecommunications or Internet companies to "maintain technical capabilities" to assist with the execution of warrants. The bill gives as one example the "removal of electronic protections" used by the company to safeguard communications or data.[11] Depending on how these provisions are applied, they could be used to undermine the security of popular Internet services, especially if they require companies to weaken encryption or redesign encrypted services to enable "back doors" or exceptional access for UK authorities.

20. Strong encryption and analogous measures designed to secure data are essential to safeguarding privacy and other rights online.[12] It is also the cornerstone of security in the digital age, shielding ordinary users from cybercrime, identify thieves, and other malicious actors. As a group of prominent computer scientists and security experts have stated, the modern world is "completely reliant on secure communications for every aspect of daily lives, from nations' critical infrastructure, to personal privacy in daily life, to all matters of business. … It is impossible to operate the commercial Internet or other widely deployed global communications network with even modest security without the use of encryption."[13] Intentionally compromising encryption, even for arguably legitimate purposes, weakens everyone's security online, not just those suspected of wrongdoing, and can put even government systems at risk.

21. Any provisions that could be interpreted to require companies to weaken secured services or build back doors into encryption raises serious human rights concerns. A requirement of either decryption or assured decryptability for all online communications, including the billions that

---

[10] Theresa May, Oral statement to Parliament, "Home Secretary: Publication of draft Investigatory Powers Bill," November 4, 2015.

[11] IP Bill Part 9, clause 189.

[12] UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, U.N. Doc. A/HRC/29/32, May 22, 2015, http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx (accessed December 21, 2015).

[13] Harold Abelson, et al., "Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications," Massachusetts Institute of Technology Computer Science and Artificial Intelligence Laboratory Technical Report, July 6, 2015, http://dspace.mit.edu/handle/1721.1/97690 (accessed December 21, 2015).

involve no suspicion of threat to public order or national security, could not be proportionate and has never been shown to be necessary.

22. *Recommendations*:
    a. The bill should be amended to ensure authorities are prohibited from imposing obligations on Internet service providers to weaken security measures or design their systems to incorporate measures for exceptional access into encryption by UK authorities.
    b. The committee should seek greater public transparency from intelligence and law enforcement agencies into how equivalent provisions have been applied under current law, and how this might change under the IP Bill.

Equipment Interference Powers Require More Scrutiny

23. The draft bill provides an explicit legal basis for equipment interference/computer network exploitation (that is, hacking), placing existing practice on firm legal footing for the first time. Hacking allows law enforcement to surreptitiously access data and communications directly from personal devices and other equipment, which can allow authorities to bypass encryption. The draft bill contemplates both targeted and bulk equipment interference, and warrants must be approved by judicial commissioners. These provisions allow authorities to compromise a broad range of equipment, beyond personal devices used by individuals suspected of a crime, and could include equipment belonging to major Internet companies. Warrants may also authorize a wide range of conduct to acquire broadly defined categories of information.

24. These capabilities raise novel technical and legal issues that deserve greater scrutiny before the bill moves forward. Hacking is a fundamentally more intrusive form of surveillance than interception or data collection. A single laptop or mobile phone routinely contains the equivalent of our personal filing cabinets, photo albums, years of correspondence, address books, banking information, shopping history, dating history, medical records, and bookshelf in one device. Hacking into a device can allow access to this data, along with the capture of passwords and real-time video or audio monitoring through the device's microphone and built-in camera. Once a device has been hacked, authorities can covertly delete or alter files and systems, or even sabotage or destroy them.

25. In addition, hacking can also cause broad and unintentional harm to devices and networks, affecting a broad range of users who are not suspects or intelligence targets. Many techniques used to compromise equipment involve identifying vulnerabilities in widely used software (e.g.,

Microsoft Word, Android) or hardware, and exploiting those vulnerabilities to install malware onto the device. If governments are permitted to hack into devices, they have no incentive to disclose vulnerabilities to the private sector so they can be fixed. These same vulnerabilities are also used by cybercriminals and other malicious actors to steal personal data for profit, so leaving them unfixed weakens security for all users.

26. Given these broader harms, we question the proportionality and necessity of equipment interference as a whole, and these concerns are even more acute for bulk equipment interference powers. The committee must elicit and publicize more evidence detailing how these powers are currently being used. Otherwise, it is difficult to assess the legitimacy of these measures.

27. ***Recommendations***:
    a. The committee should seek greater public transparency from intelligence and law enforcement agencies into how they are using equipment interference powers under current law, and how that might change under the IP Bill.
    b. The bill should be amended to more narrowly define the information and equipment that can be targeted under targeted equipment interference warrants.
    c. Bulk equipment interference powers should be removed from the bill.

Extraterritorial Impact

28. The draft bill allows certain warrants to be served extraterritorially on communications service providers located outside the UK, who must take "reasonably practicable" steps to comply. When deciding whether it is reasonably practicable to take certain steps, UK authorities will take into account whether the warrant might require the service provider to violate the laws of another jurisdiction.

29. Mutual legal assistance arrangements are used by governments, including the UK, to obtain communications or data held in other jurisdictions for the investigation or prosecution of criminal offences. To obtain access to content held by US Internet companies, for example, UK authorities generally must make requests to US authorities under an existing mutual legal assistance treaty (MLAT) since US companies are prohibited from disclosing content without a warrant meeting US standards.[14] However, the IP Bill allows UK authorities to circumvent existing mutual legal assistance arrangements that govern cross-border law enforcement requests for content by

[14] See Jennifer Daskal and Andrew K. Woods, "A New US-UK Data Sharing Treaty?" *Just Security*, June 23, 2015, https://www.justsecurity.org/24145/u-s-u-k-data-sharing-treaty/ (accessed December 21, 2015).

permitting them to serve warrants directly on companies outside the UK. This could set a deeply troubling global precedent and undermine the rule of law. It also raises issues of transparency and legal certainty in cases where such warrants present direct conflicts between the laws of the UK and other countries, as it would when seeking content of communications from US service providers.

30. At heart, the UK would be asserting jurisdiction over data held in any country by any company that provides services in the UK. This would set a dangerous precedent, one that would spark a race to the bottom for privacy as other governments would demand of companies similar access, potentially including requests for data of UK citizens by abusive governments abroad.

31. *Recommendations*:
    a. Remove clauses that allow authorities to serve warrants on communications service providers outside the UK.
    b. Work with the US and other governments to enhance existing Mutual Legal Assistance arrangements for cross-border law enforcement requests and improve their speed and efficiency, consistent with human rights requirements.

Remedy Remains Ineffective

32. The bill would provide for a new right to appeal decisions by the secretive Investigatory Powers Tribunal (IPT) before the Court of Appeal. However, it would fall short on providing the transparency so lacking in the current system.

33. The IPT, located under the Home Office, is the sole judicial body where individuals and organizations who suspect they have been under "unlawful" surveillance can file a complaint. Complainants have no access to the government's evidence nor ability to question it. They also have no access to the tribunal's deliberations nor the tribunal's rationale where complaints are rejected. Compounding these transparency issues, the bill would allow the Court of Appeal to hear appeals from the IPT wholly or partly in "closed material proceedings," which would exclude applicants and their lawyers from the hearings.

34. The bill also would not remove barriers to redress in the current system since users are never notified that they have been under surveillance, and so generally do not know to seek review at the IPT. While the newly created investigatory powers commissioner would be required to inform individuals of "serious errors" that affect them, the mere fact that an individual's fundamental

rights have been breached would not be sufficient by itself to be considered “serious” under the bill. In addition, before notice can be given, the Investigatory Powers Tribunal must agree that the error is serious and that it is in the public interest to notify affected persons. More information is needed about how these terms will be applied in practice.

35. ***Recommendations***:
    a. Require notification to individuals whose communications have been intercepted or whose data is collected to enable them to seek review and redress. Notice could be delayed until after an investigation has been closed (or longer in certain circumstances) where immediate notice would seriously jeopardize an ongoing investigation or there is an imminent risk of danger to human life. Requests to delay notification should be reviewed and authorized by independent judges.
    b. Hearings at the IPT should be open and public, unless the tribunal determines closed proceedings are necessary for national security or other legitimate purposes. Security-qualified lawyers, and where appropriate other lawyers and applicants, should be allowed to attend hearings, hear arguments, and review evidence before the court.
    c. The Investigatory Powers Commissioner and other oversight bodies should be required to inform individuals when it is determined that their rights have been breached so they can seek recourse.

Conclusion

36. Thank you for the opportunity to submit written evidence on the draft IP Bill. If we may be of any additional assistance, please do not hesitate to contact us.

###

For further information, please contact:

Cynthia Wong
Senior Internet Researcher
wongc@hrw.org

Izza Leghtas
Western Europe Researcher
leghtai@hrw.org