Joint Committee on Human Rights
Committee Office · House of Commons · London · SW1A 0AA
Tel 020 7219 4710 Email JCHR@parliament.uk Website www.parliament.uk

From Joanna Cherry KC MP

[By Email]

Home Secretary
Rt Hon James Cleverly MP

6th March 2024

Dear James,

Re: Investigatory Powers (Amendment) Bill

As you may be aware the Joint Committee on Human Rights has been undertaking legislative scrutiny of the Investigatory Powers (Amendment) Bill ("the Bill") which seeks to amend the Investigatory Powers Act 2016 ("IPA").

Firstly, I would like to thank you and your Department for the good quality documentation accompanying the Bill, as well as their assistance to the Committee staff as we have been undertaking our scrutiny of this Bill. The ECHR Memorandum rightly acknowledges that the Bill engages Article 8 (right to respect for private and family life), Article 10 (freedom of expression) and Article 1 of Protocol 1 (right to peaceful enjoyment of possessions).[1] Notably it acknowledges that in this field there must be adequate safeguards from the arbitrary exercise of powers and from any unjustified interference with fundamental rights.[2] Further, the requirement for prior judicial approval by a Judicial Commissioner (or the Investigatory Powers Commissioner) for many of the powers in the Act and the Bill gives helpful reassurance of independent oversight in ensuring that these powers are only used where necessary and proportionate to do so.[3] There are however a few points that could benefit from further clarification – whether on the face of the Bill, in undertakings to the House or in policy documents - and this letter will focus on these areas.

Notification notices & notices reviews: risks of delays to security and privacy upgrades

Clause 21 (notification of proposed changes to telecommunications services etc) (inserting new clause 258A and 258B into the IPA) makes changes to the notices regime, through the introduction of a notification notice, requiring telecommunications operators to provide prior notification of "relevant changes". Such notification notices would be subject to the requirements of being "necessary" and "proportionate" but, unlike other notices under the IPA, would not be subject to the "double lock" as they would not require Judicial Commissioner authorisation. Moreover, under changes being made in clause 18 (Review of notices by the Secretary of State) which amends section 90 of the IPA, any changes or updates that could impede the intelligence agencies' access could not be deployed pending a review of any data retention notice, technical capability notice or national security notice. Such a review would be carried out by the Secretary of State rather than an independent authority, such as a Judicial Commissioner (although the Judicial Commissioner must be consulted during a review).

---

[1] Investigatory Powers (Amendment) Bill, ECHR Memorandum.
[2] See *S and Marper v United Kingdom*; and *Big Brother Watch v United Kingdom*.
[3] See also *R (National Council of Civil Liberties) v Secretary of State for the Home Department & Others* [2023] EWCA Civ 926, (press release).

Joint Committee on Human Rights
Committee Office · House of Commons · London · SW1A 0AA
Tel 020 7219 4710 Email JCHR@parliament.uk Website www.parliament.uk

From Joanna Cherry KC MP

Nearly all of those responding to the Committee's call for evidence raised concerns that these new measures, when used in conjunction with data retention notices, technical capability notices and national security notices, could be used to delay or stop important security and privacy improvements that ought to be protecting users from online harms such as cyber-attacks, on the grounds that the Government might find the data less accessible following the updates.4 It goes without saying that secure communications protect people against cybersecurity risks, and are especially important for consumers; for politicians, doctors, or lawyers who need to protect personal data; for journalists who need to protect their sources as part of their freedom of expression rights; or for those at risk of transnational repression through digital attacks from authoritarian regimes against refugees, political dissidents, human rights activists and diaspora living in the UK.5 It is therefore clear that adequate digital security and privacy is important for the right to privacy, for freedom of expression and for the ability of human rights defenders and other democratic actors to engage fully and freely in a democracy.

There is a significant public interest in access to the best security protection online, and one which may be impeded by the reforms being deployed if the relevant Government agencies favour the interests of their own interception abilities over the interests of the public in having adequate security roll-outs on their telecommunications services. Whilst reasonable requests for timely information about changes do not seem problematic *per se*, as these new powers are not accompanied by the same safeguards as existing powers – and moreover, given that these notices are secret – there are valid questions as to whether there are adequate safeguards in place to give sufficient comfort that these expanded powers will comply with human rights and enable consumer safety and protection. It is important that there are sufficient independent safeguards (operating in good time) to prevent unjustified delays in rolling out security and privacy upgrades given the obvious potential harm this could do to end users who might otherwise be the victims of cyber-attacks, transnational repression or other online harm.

The Committee welcomes the undertaking from the Government that these new notices measures would not apply to security patches.[6] However, that is not apparent on the face of the Bill and moreover, this undertaking seemingly does not apply to all security updates only "patches". ***The Committee would like an undertaking from the Home Secretary that notice requirements would not cover, impede or delay essential security upgrades, and would ask that these guarantees – for the benefit of all in the UK – be placed on a clear legal footing, to help to improve transparency and trust in these processes.***

The Committee notes that, unlike all other notices, the proposed notification notices do not benefit from the 'double lock' of requiring the approval of a Judicial Commissioner. ***Given the level of concern at what the new notice regime could lead to, the Committee would ask the Government to consider requiring Judicial Commissioner approval for the issuing of a notification notice.***

[4] See, for example, IPA0004 (Privacy International) and IPA0005 (Internet Society, Internet Society UK England Chapter).
[5] IPA0007 (Open Rights Group); IPA0009 (Global Network Initiative), IPA0010 (techUK).
[6] The government published a policy statement in December 2023 setting out further detail regarding the intention of the regulations, including specifically that security patches are not within scope.

Joint Committee on Human Rights
Committee Office · House of Commons · London · SW1A 0AA
Tel 020 7219 4710 Email JCHR@parliament.uk Website www.parliament.uk

From Joanna Cherry KC MP

The Committee notes that concerns have been expressed that review periods could delay the roll- out of essential security and privacy improvements to online services. ***Could you please provide greater clarity on what a reasonable length of time would be for a review of a notice?***

Finally, the Committee notes concerns that the review process (which is the manner in which the subjects of notices can seek to challenge those notices) is decided by the Secretary of State, who made the original notice. ***What thought has been given to introducing an independent appeals process - such as the review being decided by a Judicial Commissioner not previously involved in any notice decision? Would such a process not be preferable from the perspective of improving the independence of appeals and thus the legitimacy of the notices system?***

Low or no reasonable expectation of privacy bulk personal datasets (Part 7A)

Clauses 1 and 2 (which inserts Part 7A into the IPA 2016), introduce a new subset of "bulk personal datasets" where there is "low or no reasonable expectation of privacy" and thus would be subject to lesser safeguards than the existing bulk personal datasets which are covered under Part 7 IPA. "All the circumstances" including a set number of "factors" would be considered in assessing whether there was "low or no reasonable expectation of privacy" in respect of a bulk personal dataset. However, those responding to the Committee's call for evidence expressed concerns that the factors focussed on the public nature of the evidence and not an individual's reasonable expectations of how their data would be processed,[7] and they challenged the notion of "low or no reasonable expectation of privacy".[8]

There is perhaps some ambiguity or confusion as to what data is envisaged to be caught by these provisions. For example, is it merely online encyclopaedias, Companies House registers or news articles; or would it also cover, for example, quite extensive discussions over the internet or mass voice or face images, as has been mentioned in evidence?[9] Discussions online often disclose sensitive information (whether about the individuals themselves or a person they are talking about) such as an individual's sexual orientation, political opinion, religion, health status or potentially sensitive information about children. The requisite clarity about the scope of these measures is currently not available from the face of the Bill. ***Greater clarity would be helpful to understand the sorts of things within and outwith the scope of this category, and in improving transparency and confidence in this process. Could you please provide this clarity as to the sorts of information that would, and would not, fall within the scope of the "low or no reasonable expectation of privacy" bulk personal dataset.***

[7] New clause 226A of the IPA 2016 (to be inserted by clause 2 of the Bill). The factors include the nature of the data; the extent to which it has been made public; the extent of the individual's consent to the data being made public; the extent of editorial control/professional standards in making it public; the extent to which it is widely known about; and the extent to which it has already been used in the public domain. See, for example, IPA0004 (Privacy International).

[8] See, for example, IPA0005 (Internet Society, Internet Society UK England Chapter) or IPA0008 (Freedom from Big Brother Watch).

[9] See, for example, IPA0004 (Privacy International), IPA0005 (Internet Society, Internet Society UK England Chapter), IPA0008 (Freedom from Big Brother Watch).

Joint Committee on Human Rights
Committee Office · House of Commons · London · SW1A 0AA
Tel 020 7219 4710 Email JCHR@parliament.uk Website www.parliament.uk

From Joanna Cherry KC MP

Could you please consider including such an indicative list within Part 7A, perhaps as an amendment to clause 226A to the IPA; this could be of great assistance and provide reassurance and confidence in this process.

Could you please clarify whether only lawfully obtained data would fall within this category, or also e.g. hacked data?

Whilst sensitive personal data, such as health data, is specifically excluded from being caught by a bulk personal dataset under Part 7 of the IPA (and is specifically addressed in relation to third party bulk personal datasets in new part 7B), such an exclusion is not present under the new Part 7A. ***It ought perhaps to be clarified on the face of the Bill that no or low expectation of privacy bulk personal datasets could not cover sensitive personal data. Can you guarantee that potentially sensitive information, such as health data, would not be caught by "low or no reasonable expectation of privacy" bulk personal datasets? Could you please explain how any such data inadvertently caught would be dealt with? Could you consider clarifying this on the face of the Bill?***

The approval of a Judicial Commissioner would still be required at either the individual authorisation or the category authorisation stage, so a level of external oversight is maintained. However, concerns have been expressed that the category authorisations are rather general in nature and could be very broad (and moreover that individual authorisations within such broad category authorisations do not need Judicial Commissioner approval).[10] More specifically, it is concerning that an individual authorisation made without Judicial Commissioner approval could continue for three months after a category authorisation to which it related has been cancelled or not renewed – one would normally assume that Judicial Commissioner approval should be immediately sought in such a case in order for the authorisation to persist. ***The Committee considers that clause 226CD should be amended to require Judicial Commissioner approval within a matter of days in cases where an individual authorisation has not received Judicial Commissioner approval and the category authorisation to which it relates lapses. Clause 226CD could, for example, replace the reference to "three months" with "three days" in clause 226CD(3), and/or insert into clause 226CD(2) "or (c) it is approved by a Judicial Commissioner within a period of three working days after the category authorisation has ceased to be in force".***

There are questions as to how children's data, within bulk personal datasets, will be protected. It does not seem that any specific analysis has been done as to the impact of these measures on children's rights. Given that children cannot give consent in the same way as adults and therefore cannot necessarily be deemed to have low or no reasonable expectation of privacy in the same way as adults, this is particularly pertinent in relation to these provisions. However, child rights ought to be borne in mind in the development of this policy as a whole.

[10] See, for example, IPA0004 (Privacy International).

Joint Committee on Human Rights
Committee Office · House of Commons · London · SW1A 0AA
Tel 020 7219 4710 Email JCHR@parliament.uk Website www.parliament.uk

From Joanna Cherry KC MP

A child rights analysis should be undertaken for all of the powers in the IPA and the Bill. This ought to have been included within the human rights memorandum prepared alongside this Bill. Could your Department please undertake this analysis and then communicate it to the Committee. This analysis should include specific consideration of the potential impact of the use of investigatory powers on children and should explain how the consideration of the specific situation and rights of children would be factored into decision-making in the use of powers under the IPA (including as amended by the Bill).

Third party bulk personal datasets

Clause 5 (inserting a new Part 7B into the IPA 2016) introduces specific provisions clarifying how warrants would be issued for the intelligence services to access "third party bulk personal datasets" in order to examine those datasets held by third parties. This warrant must be approved by a Judicial Commissioner following a personal decision by the Secretary of State and this requires that the examination of the third party personal bulk dataset be necessary and proportionate.

There are concerns that third party bulk personal datasets may themselves have been obtained or collected unlawfully – and therefore that these provisions may allow the intelligence services to access data that has been collected or processed contrary to the law.[11] Whilst the Committee understands that under Part 7B, the intelligence services will not be obtaining and storing the third party personal dataset on their own systems, as they are accessing this data there are legitimate questions to be asked as to whether that dataset has been lawfully obtained – and if not, whether additional safeguards ought to be included in any decision-making as to whether to seek a warrant to examine that dataset. ***Will the intelligence services only seek warrants in respect of third party bulk personal datasets that have been lawfully obtained? And if not, could you please consider including specific safeguards for consideration by the intelligence services and the Judicial Commissioners when contemplating granting a warrant to access unlawfully obtained third party bulk personal datasets?***

Internet Connection Records

Clause 15 (which amends s. 62 IPA 2016) extends the way that "internet connection records" (a record of when a user connects to a site or service on the internet) can be used to enable intelligence services and the National Crime Agency to search for subjects accessing e.g. a particular website, over a wider period of time. Such warrants would only be for purposes relating to national security and serious crime and would need to be authorised by the Investigatory Powers Commissioner.

Concerns were expressed by those submitting written evidence that this expansion could lead to pre-crime target detection, targeting people for association, or fishing expeditions.[12] The Committee is also aware of the Home Office documentation highlighting the usefulness of such records in e.g. highlighting people who had been accessing websites with illegal images of children, and thus in combatting child sexual exploitation online.[13]

---

[11] See, for example, IPA0004 (Privacy International), who cite the example of some data brokers; complaints to the Information Commissioner's Office in respect of data broker credit reference agency Experian; and the risks of hacked and stolen data being used in third party bulk personal datasets.
[12] See, for example, IPA0007 (Open Rights Group) or IPA0008 (Freedom from Big Brother Watch).
[13] Home Office Report on the Operation of the Investigatory Powers Act 2016, published 9 February 2023.

Joint Committee on Human Rights
Committee Office · House of Commons · London · SW1A 0AA
Tel 020 7219 4710 Email JCHR@parliament.uk Website www.parliament.uk

From Joanna Cherry KC MP

This expansion of Internet connection records powers will need careful oversight and constraint. It will be important that the Investigatory Powers Commissioner's annual reports to the Prime Minister, laid before Parliament, adequately cover any potential errors or abuses in the use of these enlarged internet connection records powers, so as to ensure that such powers are only being used appropriately, where it is truly necessary and proportionate to do so - and to ensure that individuals improperly affected are informed so that appropriate action can be taken.

I would be grateful for a reply by 20 March 2024.

I will send a copy of this letter to the Chair of the Home Affairs Select Committee.

Yours sincerely,

Joanna Cherry KC MP

Chair, Joint Committee on Human Rights