Revisions to the Investigatory Powers Act 2016

Response to Call for Evidence from the Joint Committee on Human Rights

Internet Society and Internet Society UK England Chapter

January 2024

Summary

The Internet Society submitted a response[1] to the initial consultation on the IPAB, in June 2023, setting out a broad range of concerns about potentially harmful effects of the proposals. Those concerns persist and include harmful impact on the security of the Internet. For the purposes of this briefing document, we have limited our input to two parts of the Bill that most directly threaten human rights:

1. The creation of Secretary of State powers to prevent technology companies from deploying new or improved security functions in digital products and services.
2. The mischaracterisation of bulk personal datasets (BPDs) as "data in which the individual has no, or low, expectations of privacy.

We also voice concern over procedure as the Report Stage hearing is scheduled for 23 January, just one day after the deadline for this call for evidence. We question the Joint Committee's ability to process submissions and provide input to the policymaking process with such tight deadlines, risking insufficient diligence when it comes to human rights implications.

Recommendations

We recommend that the Committee put forward the following amendments:

1	to **include explicit safeguards (such as a prohibition on systemic vulnerabilities)** to prevent unsafe use of the resulting powers.
2	to require that **impact assessments on fundamental rights and privacy** are conducted and properly reflect the legitimate interests of all stakeholders.
3	to **prohibit the issuing of notices that would allow general monitoring.**

[1] "The Revised IPA 2016 Consultation Response." *Internet Society UK*, 31 July 2023, isoc-e.org/the-revised-ipa-2016-consultation-response/.

4	to require that **Internet impact assessments** are conducted for this revision, given the intersection between critical properties of the Internet and the exercise of human rights.
5.1	to ensure that **operators are not required to comply with a notice until objections to it have been resolved**.
5.2	to ensure that **objections made by an operator go through an independent appeals process**.
5.3	To ensure that **any revision of the IPA demonstrates how its operation and enforcement will comply with the necessity and proportionality requirements.**

Powers established by the proposed changes:

The Internet Society notes the creation of the following new Secretary of State powers:

- to require that an operator delay making changes (and, by implication, security improvements) to their system while an objection lodged by the operator is being reviewed.
- to require that operators give advance notice of changes to their systems, or of their intent to operate a service.

Need for comprehensive impact assessments

The Internet Society stresses the importance of comprehensive impact assessments across a range of factors. We note that legislation in related areas, including the Online Safety Bill, has been based on incomplete impact assessments, and in some cases has been struck down by the courts[2].

Systemic impact on online safety

New powers created by the bill amount to pre-emptive government interference in the development process for product, application, and service security. This should worry us, given the history of such interference resulting in systemic and deliberate flaws in product security[3]. Creating the power for the Government to insist on approving technical innovation is a dangerous and retrograde step, which runs counter to all industry norms for product security.

New powers seek to impose the equivalent of licensing requirements on service providers, and to do so for the purposes of law enforcement objectives, not user security, privacy, safety, or exercise of human rights. It will put law enforcement in the position of deciding what technologies can or cannot be used or deployed in the UK, a situation that goes far beyond the scope of law enforcement's role in society. It will also leave citizens at greater risk, as service providers may decide there is no point

[2] "Q&A: Privacy International - UK High Court Judgment." Privacy International, privacyinternational.org/frequently-asked-questions/4360/qa-privacy-international-uk-high-court-judgment. Accessed 31 July 2023.

[3] "BSAFE." Wikipedia, 7 June 2023, en.wikipedia.org/wiki/BSAFE.

incurring the cost of developing new and better security measures, if these can simply be rejected by the Secretary of State.

Security flaws in consumer products and services not only put citizens' data at risk, they also compromise people's physical safety and ability to exercise their human rights. Indeed, the Australian TOLA legislation repeatedly and explicitly *prohibits* the use of its powers to compel operators to introduce a "systemic weakness" or "systemic vulnerability"; the proposed revisions to the IPA do not mention such a safeguard.

New powers also create the possibility of a general equipment interference capability, which we believe is contrary to the UK High Court judgment.[4] Such interference risks making the United Kingdom the weak link in the Internet's security and trustworthiness, undermining the Internet as a global infrastructure, and putting individuals and their fundamental rights at greater risk both within and beyond the UK.

Impact on fundamental rights

Bulk interference with equipment and communications

In his August 2016 Report of the Bulk Powers Review, David (now Lord) Anderson noted the danger of overly broad warrants for interference:

> *'I have previously commented that the widely drawn provision for targeted thematic EI [equipment interference] "effectively imports an alternative means of performing bulk EI, with fewer safeguards" '*

In 2021, the High Court judgment[5] on the Intelligence Services Act 1994 ruled against the use of "general warrants" to authorise interference with devices and communications.

We believe that new powers under the bill amount, similarly, to an alternative means of performing bulk equipment interference, by empowering the Government to direct the design, pre-emptively, of products and services intended for the UK consumer market.

Privacy impact of bulk personal datasets

In an increasingly digital society, it is essential that citizens robustly secure their data and communications to reduce their risk of harm. Personal data that is sensitive in one context may not be sensitive in another context. There are few examples of personal data where a user has "no or low" expectations of privacy.

---

[4] "Q&A: Pi Case - UK High Court Judgment on General Warrants and Government Hacking Explained." Privacy International, 8 Jan. 2021, privacyinternational.org/long-read/4361/qa-pi-case-uk-high-court-judgment-general-warrants-and-government-hacking-explained.

[5] "Q&A: Privacy International - UK High Court Judgment." Privacy International, privacyinternational.org/frequently-asked-questions/4360/qa-privacy-international-uk-high-court-judgment. Accessed 31 July 2023.

The Independent Review of the IPA (published in June 2023) describes the rapid proliferation of personal data as a problem for law enforcement that can be solved by relaxing regulation of the collection and use of Bulk Personal Datasets (BPDs). Yet the same Review acknowledges "the possibility that most data referencing human activity can in theory be resolved to real world identities". Lord Anderson seeks to allay this tension by stating that *relaxing* safeguards is the best solution given that for BPDs "there is a low or no expectation of privacy".

First, given his own acknowledgement that "most data referencing human activity can in theory be resolved to real world identities", we respectfully disagree.

Second, we believe that the policy rationale on bulk personal datasets is based on a misunderstanding of the contextual nature of privacy. Data that is not contentious in one context may be highly contentious if shared or used outside that context. We believe there are now few, if any, instances of personal data in which an individual has "no or low" expectation of privacy *regardless of the context in which that data is shared or used*.

There is no informed policy debate on this question because there is a grave lack of transparency about which datasets BPDs are, and therefore what contextual privacy expectations individuals may legitimately have in their regard.

Governance-related risks

Perverse incentives

Under new powers an operator would be obliged to comply with a notice to which it believes it has a legitimate objection, even while that objection remains unresolved. This creates a perverse incentive for the Secretary of State to delay resolution of the objection. If the operator's objection were to be upheld, the status of data collected in the meantime is unclear.

Accountability concerns

Review of an operator's objection by the Secretary of State runs the risk of failing to be impartial, given that it is the Secretary of State who issued the notice in the first place (presumably believing there are solid grounds for doing so).

Changes to the IPA must be viewed in the context of previous regulation of interception and surveillance powers, particularly the well documented misuse of RIPA powers to investigate minor offences with no element of terrorism or national security.[6] Any amendments to current powers must include explicit safeguards against "scope creep" and inappropriate extension of powers through secondary legislation.

[6] Asthana , Anushka. "Revealed: British Councils Used Ripa to Secretly Spy on Public." The Guardian, 25 Dec. 2016, www.theguardian.com/world/2016/dec/25/british-councils-used-investigatory-powers-ripa-to-secretly-spy-on-public.

Conclusions and recommendations

1 – The proposed amendments to the Investigatory Power Act 2016 are premature, and not sufficiently justified.

New powers established by the bill have the potential for high impact on the security and privacy of UK citizens and their devices, communications, and data. This would directly threaten some rights, such as the right to privacy. For vulnerable individuals and communities in particular, a lack of access to confidential communication also represents a serious threat to freedom of association and freedom of expression.

Recommendation 1: that the Committee **put forward amendments for explicit safeguards (such as a prohibition on systemic vulnerabilities)** to ensure that the powers are not used to undermine the privacy, security, and safety of innocent users to the detriment of their ability to exercise human rights.

2 – Current impact assessments are inadequate

The proposed changes, and the Independent Reviewer's recommendation on looser regulations for BPDs, give rise to significant concerns relating to privacy and personal safety. The Review places great weight on the impact on law enforcement but does not give similar weight to the potential impact that new powers could have on citizens' rights, in our increasingly online lives.

Recommendation 2: that the Committee **put forward amendments to require that revision of the IPA 2016 be conditional on an assessment of its impact on privacy and other fundamental rights**, to ensure that the legitimate interests of all stakeholders are properly addressed and are not put at risk by systemic vulnerabilities.

3 - Consentless general monitoring represents a systemic vulnerability and fails the proportionality test by definition.

Notices which have this outcome introduce systemic insecurity in mass market technology, and therefore create significant threats to cybersecurity, and individual privacy and safety.

Recommendation 3: that the Committee should **put forward amendments that prohibit the issuing of notices that make general monitoring possible.** This prohibition should apply equally to:

I. **Notices that oblige an operator to deploy technology** that makes general monitoring possible.

II. **Notices that prevent an operator from removing or remedying an existing function** that makes general monitoring possible.

4 - Internet impact assessment

The proposed revisions have implications for the Internet's security and correct functioning. They enable Government interference in the design and development of product security and would allow

the IPA to result in the same outcomes as forms of warrantry that have already been ruled unlawful. The Government should be contributing to improved security of the global Internet infrastructure, not undermining it, not least for the interconnection between security, trust, and the exercise of human rights.

Recommendation 4: that the Committee **request an independent Internet Impact Assessment**[7] of any proposals to amend the IPA 2016.

5 – The need for sufficient safeguards for use of the proposed powers

As currently described, the proposed changes create a perverse incentive for the Secretary of State to issue an order and then delay processing any appeal against that order.

Current accountability and transparency processes for the IPA fail to address the necessity and proportionality criteria, and the consultation document does not explain how that would be remedied. We recommend that the Committee put forward amendments to ensure:

Recommendation 5.1: that operators are not obliged to comply with a notice until objections to it have been resolved.

Recommendation 5.2: that objections go through an independent appeals process.

Recommendation 5.3: that any revision of the IPA demonstrate how its operation and enforcement will comply with necessity and proportionality requirements.

[7] "Internet Impact Assessment Toolkit." Internet Society, 31 Oct. 2022, www.internetsociety.org/issues/internet-way-of-networking/internet-impact-assessment-toolkit/.