Revisions to the Investigatory Powers Act 2016

Internet Society and Internet Society UK England Chapter - consultation response

31st July 2023

Summary

The Internet Society is concerned by the proposed revisions to the Investigatory Powers Act 2016, because of the intrusive nature of new powers they would establish, and their impact on the digital economy, online trust, and fundamental rights. We maintain that the Investigatory Powers Act cannot be effectively evaluated in isolation from the Online Safety Bill, given that the latter also creates new obligations relating to the design, governance, and security of communication services.

Please find our high-level recommendations below, followed by more detailed analysis.

Recommendations

1.1	That **this public consultation take place only after the passage of the Online Safety Bill**, given their interrelated nature.
1.2	That the re-issued public consultation **include proposals for explicit safeguards (such as a prohibition on systemic vulnerabilities)** to prevent unsafe use of the resulting powers.
2.1	That **economic impact assessments** are conducted for both this revision and the Online Safety Bill.
2.2	That **Internet impact assessments** are conducted for this revision.
2.3.1	That Government **prohibit the issuing of notices that would allow general monitoring**.
2.3.2	That **impact assessments on fundamental rights and privacy** are conducted before any revision, and properly reflect the legitimate interests of all stakeholders.
3.1	That **operators are not required to comply with a notice until objections to it have been resolved**.
3.2	That **objections made by an operator should go through an independent appeals process**.
3.3	That any revision of the IPA should **set out how its operation will be shown to meet the necessity and proportionality criteria.**

Table of Contents

Powers established by the proposed changes:

The Internet Society contests the claim made in paragraph 1 of the Ministerial Foreword, stating that "this consultation is not about the creation of new powers". We see the creation of new powers in the following ways:

- Objective 1 gives the Secretary of State the power 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.
- Objective 2 gives the Secretary of State the power to require that an operator co-operate with a consultation process, share technical information about proposed changes, and do so in a timely manner.
- Objective 3 proposes to introduce stronger penalties for non-compliance with the notices regimes.
- Objective 4 introduces a power for the Secretary of State to require operators to 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[1].

Economic impact assessment

The proposed changes to the IPA represent a threat to confidential business communication, which would put every UK business at risk, undermining the security of UK businesses and their transactions. This in turn would cause a crisis of confidence in UK companies being able to carry out their business on the Internet, eroding trust in the UK as a supplier of services and technical products.

In 2020, the Internet Society commissioned an independent economic impact assessment of the Telecoms and Other Legislation Amendment (Australia, 2018), TOLA for short. At the time, the researchers found no economic impact analyses for TOLA, the IPA 2016, or other countries' legislation with similar effects on the deployment of digital security technology[2].

[1] "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.

[2] "New Study Finds Australia's TOLA Law Poses Long-Term Risks to Australian Economy." Internet Society, 19 July 2021, www.internetsociety.org/news/press-releases/2021/new-study-finds-australias-tola-law-poses-long-term-risks-to-australian-economy/.

The study concluded that the negative economic impact of measures *less* intrusive than those proposed in the UK's Online Safety Bill would run into multiple billions. One Australian service provider alone estimated the actual, direct negative impact on its business at around $AUS 1 billion.

According to the study, the greatest economic risk posed by the TOLA Act is the threat it represents to public trust in digital services, including the Internet. The global economy depends on digital technology and services to such an extent that distrust in data security can have long-lasting adverse effects on a country's economy, across all industries and sectors.

The Internet Society encourages the UK Government to commission and publish a comprehensive economic impact assessment for the Online Safety Bill and any proposed revisions to the Investigatory Powers Act.

Impact on a secure and trustworthy Internet

Objective 4 gives significant cause for concern. It amounts to pre-emptive government interference in the product development process for 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 would be a step backwards.

In doing so, Objective 4 is effectively seeking 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 and safety. 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 incurring the cost of developing new and better security measures, if these can simply be rejected by the Secretary of State.

The digital era is characterised by our reliance on connected technology in particular, including digital products that have physical effect – such as connected home security systems, connected vehicles, and connected children's toys. Security flaws in consumer products and services now not only put citizens' data at risk, they compromise people's physical safety. 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.

As noted under "Bulk interference with equipment and communications", Objective 4 also creates the possibility of a general equipment interference capability, which we believe is contrary to the UK High Court cited[4]. Such interference risks making the UK the weak link in the Internet's security and

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

[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.

trustworthiness, undermining the Internet as a global infrastructure, and introducing a further drag on the UK's economic growth.

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 the powers proposed under Objective 4 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.

Bulk personal data

The Ministerial Foreword refers to "the legitimate interest in increased privacy of the majority of our citizens" and notes the exponential growth in personal data—including personal data being held overseas and in the hands of third parties. The Foreword, however, fails to conclude that, in a digital society, citizens are now more at risk as a result, if they cannot robustly secure their data and communications.

In fact, according to the Independent Review of the IPA (published in June 2023) the explosion of data is a problem for law enforcement, and should be addressed by relaxing regulation of the collection and use of Bulk Personal Datasets (BPDs):

> *'The exceptional growth in volume and types of data across all sectors of society globally since the Act has entered into force has impacted UKIC's ability to work and collaborate at the necessary operational pace. The BPD safeguards in the current statutory framework are disproportionate for some types of data, creating a negative impact on operational agility, while also*

[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.

> *harming capability development."*
> *– 3.24, Independent Review of the IPA 2016*

But the same Review acknowledged that the 2016 Act did not foresee "the possibility that most data referencing human activity can in theory be resolved to real world identities, rendering datasets that would not previously have been considered BPD [Bulk Personal Data] within the scope of Part 7 of the Act". (Part 7 governs what an intelligence service may do with a bulk personal dataset when the BPD 'includes "personal data" relating to a number of individuals.)

Lord Anderson concludes that the solution is to relax the safeguards for BPDs "in respect of which there is a low or no expectation of privacy". Given his own acknowledgement that "most data referencing human activity can in theory be resolved to real world identities", we respectfully disagree.

If anything, his concerns about "operational pace and agility" represent an argument for improved operational capability, not for reduced safeguards on personal data.

Governance-related risks

Perverse incentives

Under Objective 1, 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).

Further, the claimed justification for the power is incomplete, on the basis of the following text: "Where an operator is seeking to make changes to their system that would have a detrimental effect on a current lawful access capability…". This fails to make clear what powers and/or constraints apply, in cases where the Secretary of State issues a notice in the absence of such changes—for instance, on the establishment of a new operator.

Under Objective 4, the consultation paper acknowledges "the need for strong safeguards that deliver the IPA's fundamental principle of necessity and proportionality" — but it does not suggest how that would be achieved, or what criteria would be used. When we look at current practice, the Report on the Operation of the Investigatory Powers Act 2016, which the Secretary of State cites at the outset, explicitly ruled out assessing or offering any opinion on the proportionality of the IPA. This has created a shortfall in transparency and accountability in the operation of the IPA, to which the proposed changes do not offer a remedy.

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.

Our assessment is therefore that several areas of the consultation request lack sufficient information to show that the powers it establishes would be safe, either in principle or in practice.

Conclusions and recommendations

1 – The proposed revisions to the Investigatory Power Act 2016 are premature, and not sufficiently justified by the analysis in the consultation request.

The proposed revisions do indeed establish new powers, and several of them are intrusive, with the potential for high impact on security, fundamental rights, online trust, and the digital economy. If put into practice, the changes would pose serious risks to the security and privacy of UK citizens, their devices, communications, and data.

The Investigatory Powers Act cannot be evaluated in isolation from the Online Safety Bill, since the latter not only proposes obligations relating to the design, governance, and security of communication services, but is also still being amended by the Government, and is based on incomplete impact analyses. It is therefore premature to contemplate changes to the IPA, while so many related powers in the Online Safety Bill are still not finalised.

> **Recommendation 1.1: reissue a consultation on revision of the IPA 2016 *after* the Online Safety Bill is finalised.**
>
> **Recommendation 1.2: include proposals 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.**

2 – Current impact assessments are inadequate

2.1 Economic impact assessment

Impact assessments for both the Online Safety Bill and the Investigatory Powers Act are incomplete.

> **Recommendation 2.1: any revision of the IPA 2016 should be preceded by a comprehensive economic impact assessment that takes into account changes in the digital economy since 2016.**

---

[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.

2.2 Assessment of impact on privacy and other fundamental rights

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. Online services, connected society and the digital economy have evolved significantly since the enactment of the Investigatory Powers Act, and while the consultation considers the resulting impact on law enforcement, it does not give similar weight to the potential impact that new powers could have on citizens' rights, in this new digital environment.

> **Recommendation 2.2.1: any revision of the IPA 2016 should be preceded by a comprehensive and forward-looking assessment of its impact on privacy and other fundamental rights, to ensure that the legitimate interests of all stakeholders are properly addressed, not just law enforcement.**

Consentless general monitoring represents a systemic vulnerability and fails the proportionality test by definition. Notices which have this outcome introduce systemic weaknesses in mass market technology, and therefore create significant threats to cybersecurity, and individual privacy and safety.

> **Recommendation 2.2.2: the Government should prohibit the use of notices to 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.**

2.3 Internet impact assessment

At the core of the IPA are online services that use the Internet, and on which all UK citizens rely. 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.

> **Recommendation 2.3: procure and publish an independent Internet Impact Assessment[7] of any proposals to amend the IPA 2016.**

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

3 – The consultation request lacks detail about safe 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.

> Recommendation 3.1: operators should not be obliged to comply with a notice until objections to it have been resolved.
>
> Recommendation 3.2: such objections should go through an independent appeals process.
>
> Recommendation 3.3: any revision of the IPA should set out how its operation is demonstrated to meet the necessity and proportionality criteria.