

ISPA response to Home Office Consultation on Investigatory Powers Act amendments

Introduction

1. ISPA welcomes the opportunity to respond to this consultation and appreciates the fact that views are being sought via a public consultation exercise. We understand the importance of communications data to law enforcement and the intelligence agencies and have a shared goal of a targeted, proportionate and clear framework, one that gives our members legal certainty and minimises intrusiveness.
2. The legislative framework in this area has long been contentious and the passage of data retention powers has been fraught with challenges over the years. During the passing of the Investigatory Powers Act (the “Act”), we, and others, called for a legal framework that would comply with existing rights and rulings and so would need not be revisited on a regular basis. We therefore feel it is imperative that the Government strives to establish a robust framework, one that fully and unambiguously meets the requirements of the court judgment. It is neither in the interest of our members, nor public authorities, for this issue to be constantly revisited.
3. We are encouraged to see Government revise the communications data retention framework in light of the European Court of Justice (“CJEU”) ruling. However, we are concerned that the proposed reforms may not go far enough to address the CJEU’s judgment, leaving open the possibility of future challenges and further changes to the regime.

National security

4. We understand that there is a separate legal challenge waiting to be heard in relation to national security and the use of bulk powers and so the proposed changes to the Act following the judgment are in relation to data retention alone. Future legal challenges are likely to help clarify jurisdiction over national security policy and ISPA has no view at this stage.
5. What may additionally impact on this scenario is that in leaving the European Union, the UK will become a third country and the defence of national security being a national competency and not subject to the jurisdiction of the Court will no longer apply. In order to seek adequacy with the EU on data sharing, the UK may have to abide by decisions made by the CJEU, for example. Ensuring continued smooth uninterrupted data flows post-Brexit is extremely important, and we consider that addressing the court judgment to the fullest degree now would go a considerable way in meeting adequacy concerns at an early stage. This would bring confidence to the UK tech industry, which may otherwise be concerned by the risk of further challenge.
6. We support Government’s interpretation that the judgment ruling should not apply to data being held for business purposes. There are existing protection and standards that our members adhere to.

Additional safeguards

7. Appropriate safeguards will be key to meeting the court's requirement of a targeted regime. We therefore support further steps to make the notice regime targeted, clearer and proportionate to the associated impact upon privacy, yet there are questions as to how this would work in practice. For example, our members are unclear as to how geographical retention would work, similarly limiting retention to certain groups of customers also sounds highly challenging on a practical level and could require substantial cost and time to implement. Our members need further clarification around these points.
8. A further safeguard proposed is that of the serious crime threshold. Set at offences for which an adult is capable of receiving six months or more in prison, the definition sets a low threshold. In keeping with the aim of clearly addressing the court's concerns, we feel that Government should carefully consider whether the definition fully meets that of serious crime.
9. We understand that the court was looking at pre-Investigatory Powers Act definitions of traffic and location data rather than 'events' and 'entity' data. ISPA has no view as to whether this approach is in keeping with the judgment, but it seems questionable and open to further challenge. Clarity regarding which forms of data are relevant to the act would also assist operators in preparing to comply. In addition, we feel there should be a consistent authorisation regime for communications data requests. An approach that applies to different levels of communications data fails to meet this and adds a further degree of complexity.

Notifying targets

10. The judgment makes clear that users subject to unlawful communications data requests should be notified by the competent authorities to provide an opportunity to seek redress. We understand that Government is trying to balance competing priorities and the impact on investigations. However, we feel that to unambiguously comply with the judgment, Government may need to go beyond its proposed approach of relying solely on the Investigatory Powers Commissioner. We would welcome further clarity from Government on how its proposed approach meets the judgement.
11. As referenced in the consultation, notification is a sensitive area. Government should therefore make clear that only competent authorities will be expected to have a role in notifying users. CSPs should categorically not be expected to notify users as to whether they have been subject to investigatory powers, not least as retention notices are subject to secrecy clauses. Again, we would welcome further clarity from Government on this including explicitly referencing in the draft regulations.

Independent authorisation

12. One of the judgment's main findings is that a court or an independent administrative body has to approve access to retained communications data. Government has determined a three-tier approach of independent authorisation, internal authorisation for emergency requests and internal authorisation for intelligence and security services.

13. We welcome the introduction of an independent administrative body to approve requests. This is a step many have been calling for to strengthen safeguards. In establishing the OCDA it will be important for existing safeguards, such as the SPOC system, to be replicated. We also stress the importance of ensuring that the OCDA is sufficiently resourced, independent, and has sufficient expertise to carry out its functions effectively.
14. We understand the need for emergency authorisation. However, ISPA members would welcome additional guidance from the Home Office on the process by which urgent requests can be authorised, what actually determines an urgent request and the level of urgent requests expected. Fully clarity and certainty is particularly important where such requests are time-sensitive.

Conclusion

15. ISPA is pleased that the Home Office response to the CJEU's judgement proposes a number of important amendments to the UK's authorisation regime. However, where highlighted above, there are several areas where we feel the Government should go further to fully and unambiguously meet the requirements of the court judgment. A failure to do so could lead to a situation in the near future where the UK's regime is open to further challenge and has to be revisited once more.