Comparison of internet connection records in the Investigatory Powers Bill with Danish Internet Session Logging legislation

> We consider that, on balance, there is a case for Internet Connection Records as an important tool for law enforcement. *(Report of the Joint Committee on the Draft Investigatory Powers Bill, recommendation 12)*
>
> The Committee acknowledges that there are important differences between the ICR proposal in the draft Bill and the system which was used in Denmark. We believe that the Home Office has learned lessons from the Danish model that will increase the chances of ICRs being effective. *(Report of the Joint Committee on the Draft Investigatory Powers Bill, recommendation 19)*

1. The Investigatory Powers Bill provides for the retention of internet connection records (ICRs). This essential new power will be invaluable to law enforcement, including to prevent and detect crime, and to protect our national security. As an ever greater proportion of activity takes place over the internet, ICRs will be crucial to identifying individuals associated with known online activity and in identifying the services that a suspect or victim has used.

2. Three parliamentary committees provided thorough scrutiny of the draft Bill and we welcome the focus they have placed on internet connection records. We recognise the importance of establishing appropriate definitions and safeguards for this new power and the need to continue to build confidence in the feasibility of the proposals through collaboration with industry.

3. It is also vital that we learn from other relevant experience. Denmark previously enacted legislation with similar aims to those provided for by ICR retention, but subsequently withdrew it. The Joint Committee on the Draft Investigatory Powers Bill recognised that there are important differences between the Government's proposal for retention of internet connection records and the internet session logging model implemented in Denmark. This paper responds specifically to their recommendation that the Government should publish a full assessment of the differences between our proposal and the model tried in Denmark.

History of related legislation

4. The Investigatory Powers Bill provides for the retention of internet connection records. An ICR is a record of an event held by a telecommunications operator (CSP) about the service which one of their customer's devices has connected to on the internet. An ICR will only identify the service that a customer has been using, it is not intended to show what a customer has been doing on that service.

5. ICRs will be generated by CSP from communications data available in their networks. There is no single set of data that constitutes an ICR, it will depend on the service provider and service concerned. However the core information will include source and destination internet protocol (IP) addresses and ports, time/date and an account identifier. They may include additional information such as the service identifier, URL domain name, and volume of data transferred.[1]

6. CSPs will only be required to retain ICRs when they have been issued with a data retention notice requiring them to do so following a period of consultation.

7. The Danish data retention legislation, which took effect in 2007, included session logging requirements for internet traffic by fixed and mobile network operators. While this was intended to achieve similar objectives to the powers outlined above, there were a number of significant differences in the Danish approach which reduced the effectiveness of the capability that was implemented.

8. The Danish legislation was withdrawn in 2014 following an evaluation by the Danish Ministry of Justice[2] which identified issues with the way that the capability had been implemented by CSPs and the utility of the resulting data. The Danish Ministry of Justice has indicated that session logging could be reintroduced if the technical problems can be properly addressed.

9. The Government has, and will continue to, consult widely to ensure that the legislation is implemented as effectively as possible in order to provide maximum operational benefit. We have spoken to individuals with first-hand experience of the Danish legislation and its implementation in order to ensure all possible lessons are learnt. The result is a Bill and proposed implementation approach which has taken into account a number of important factors in its approach to ICRs, as follows:

---

1 More detail on the construction of an ICR can be found in 'What is an Internet Connection Record?' on the Joint Committee on the Draft Investigatory Powers Bill webpage at www.parliament.uk under Home Office written evidence (IPB0146), published 14 January 2016.

2 Data retention evaluation report, Danish Ministry of Justice (in Danish) http://www.ft.dk/samling/20121/almdel/reu/bilag/125/1200765.pdf

- **Technology neutral legislation:** Maintaining a technology neutral approach on the face of the Bill itself so that solutions can be developed in partnership with individual CSPs as appropriate.
- **CSP cost recovery:** Providing recovery of all reasonable costs to CSPs so that an appropriate balance can be achieved between the technical design of an individual CSP's system and the required operational benefits.
- **Linking data to customer accounts:** Ensuring that data is collected at appropriate points in the network, and in such a manner so as to enable IP addresses to be tied back to specific customer accounts.
- **Representative data collection:** Ensuring that the use of techniques to reduce the volume of data, such as data sampling, do not undermine the accuracy or utility of retained data.
- **Collecting adequate information:** Ensuring that the definition of ICRs in the Bill enables the collection of relevant communications data that would assist in identifying the internet service accessed.
- **Uplifting end user skills and tools:** Ensuring the law enforcement organisations have the expertise and tools necessary to enable them to use the data effectively and efficiently.

Comparison of proposals for retention of ICRs

10. An analysis of each of the areas outlined above, including differences between the Danish approach and the provisions providing for retention of ICRs in the Investigatory Powers Bill, is provided in the following sections.

Technology neutral legislation

11. The Danish session logging legislation specified two implementation options. CSPs could either:
    - retain the first and last packet of each session within their network; or
    - conduct sampling by retaining every 500th packet of a user's communication at the boundaries of their network.

12. The Danish authorities' original requirement was to retain the first and last packet of each session as this was considered to provide the most accurate representation of customers' internet activity. However the major CSPs were concerned about the level of investment that this would require them to make. The second option was therefore included in legislation allowing for simplified data collection (for example by removing any need for deep packet inspection) and reduced data volumes and storage costs.

13. In the UK, the Investigatory Powers Bill has sought to strike a careful balance between the detail required to provide appropriate transparency of legislation

and the technical neutrality required to ensure that the Bill remains valid in a world of rapidly evolving technology. The Bill itself does not therefore specify how ICRs should be implemented.

14. This further allows the Government to give space to its key principle of developing tailored solutions in close consultation with CSPs to ensure that outcomes are achieved whilst maintaining cost effectiveness. Further guidance is included in the draft Communications Data Code of Practice which will be published at introduction. Specific requirements will be set out in individual retention notices so that they can be tailored to each CSP and aligned with operational priorities.

15. In addition, before a notice is issued, benefit is balanced against feasibility for the CSP and cost. If, after this consultation process the Government decides to issue the retention notice but the CSP considers that a retention notice is not practicable, the Bill provides a clear route for CSPs to appeal to the Secretary of State. In considering their appeal, the Secretary of State must take advice from the Technical Advisory Board (TAB) on costs and technical feasibility and from the Investigatory Powers Commissioner (IPC) on proportionality.

CSP cost recovery

16. In Denmark, CSPs are required to meet the implementation costs of retention systems and are then paid for their subsequent use. As noted above, CSP concerns about the costs that they would bear in relation to internet session logging systems influenced the decision to include the sampling implementation option in Danish legislation, and indeed this was the option that was subsequently implemented by the majority of CSPs.

17. The fact that the CSPs funded the implementation of their solutions may also have reduced the visibility and influence that the Danish authorities had over the CSP's logging solution designs and implementation choices.

18. In the UK, government policy is to fund 100% of the reasonable costs incurred by CSPs in complying with communications data retention notices. This means that CSPs are not financially disadvantaged by compliance and are not incentivised to pursue lowest cost solutions. This arrangement enables the Secretary of State to achieve an appropriate balance between operational benefits and the cost of CSP compliance solutions.

19. In doing so, the government also works closely with CSPs and operational partners before and during implementation to ensure that the solutions are capable of meeting operational requirements and are cost effective.

Linking data to customer accounts

20. The most widely implemented option in Denmark involved collecting data at the boundary of CSP's networks. This is the point in the network furthest away from data about the customer and therefore some elements of the collected information would have been difficult for investigators and analysts to utilise effectively.

21. In particular the data would be captured after IP Network and Port Address Translation (NAT / PAT) had been applied[3]. This changes the originating address of each packet and means that the source IP address no longer uniquely identifies an individual customer unless the port number is also known. As a result Danish investigators trying to identify a customer associated with a known online activity would have needed to know port information which is often not available from service providers and server logs. They would also have needed CSPs to retain and process NAT/PAT logs to resolve the translated address back to a customer account.

22. The absence of a clear and readily available link between session log data disclosed by the CSP and customer account data would also have made it very difficult for Danish investigators to conduct analysis where their starting point was a particular customer or customer device.

23. The choice of data collection point and lack of ability to link the data to individual customers in Denmark therefore severely limited the value of data collected from CSPs which share IP addresses across customers – predominantly mobile CSPs. This would have undermined the ability to utilise this capability in relation to smart phones and other mobile data services in particular.

24. In the UK, the Investigatory Powers Bill does not specify where in a network data should be captured - instead leaving this to the detailed requirements in individual CSP retention notices. The Home Office is already working with CSPs to ensure that they are able to log the information required for linking IP addresses to customer accounts under the Counter Terrorism and Security Act 2015.

Representative data collection

25. In Denmark, the solution to session logging selected by the majority of CSPs involved sampling every 500th packet at the network boundary. Although the legislation required sampling per user, in a number of cases this appears to

[3] Carrier Grade NAT/PAT can result in thousands of users sharing a single IP address at any point in time and a single user's IP address changing by minute or even seconds. NAT/PAT is widely used in mobile networks and in some fixed networks

have been implemented as sampling across all user traffic, potentially comprising thousands of users at a sampling point. This would make it very difficult to reconstruct a coherent understanding of an individual user's activity, as the data which might happen to be collected for that user would be highly unpredictable and significant activity could be missed completely[4].

26. This approach to sampling is also closely related to the overall volume of data users are generating rather than the number of user activities or events. So, for example, as more messages include images or video clips, the size of each message will increase but there would not necessarily be more messages. This could therefore have resulted in a more rapid growth in sampled data volumes than if the sampling were linked to user activity.

27. The manner of implementation would have limited the value of data available from both mobile and fixed line services.

28. The Investigatory Powers Bill does not specify any sampling constraints or requirements in relation to the retention of ICRs. It is possible that, following joint design work with individual CSPs, some ICR implementations may involve sampling. However this will be subject to thorough evaluation in order to ensure that the retained data is still capable of meeting operational requirements.

Collecting adequate information

29. Danish legislation specified that session logs should include the source and destination IP addresses and ports, transport protocol and timestamp when the sampling option was implemented. It did not require the retention of any additional information that could help in identifying the actual internet service being used. As the destination IP address does not always map uniquely to a service this would have made the crucial information for an investigation – what service was a customer making use of – more difficult to identify.

30. The definitions in the Investigatory Powers Bill provide flexibility for ICRs to include additional communications data. This can include some domain names and other service identifiers where they are available to the CSP and necessary to provide operationally useful data. Additional detailed information about the data that could comprise ICRs is provided in the draft Communications Data Code of Practice which will be published alongside the Investigatory Powers Bill. Specific data and processing requirements will be

[4] If 1000 users' traffic was passing through a sampling point and each user generated a similar amount of data, then a 1:500 sample across all traffic would result in an effective sampling rate for each individual user of one in 500,000 packets. Assuming an average IP packet size of 500 bytes, this would mean that a user might transfer up to 250MB without any log being created. This would be consistent with, for example, over fifty 30 second video clips. Even if the sampling rate were increased there would be no guarantee that an individual's activity would be effectively captured.

developed in consultation with individual CSPs taking account of their network architecture and operational requirements, and will be included in individual retention notices.

Uplifting end user skills and tools

31. The Danish system for law enforcement organisations to access communications data held by CSPs relied on the data being provided in a standard format. This system was not fully functional until 2010, some four years after session logging was first implemented. This system did not then provide the capabilities that were needed by the law enforcement organisations to analyse the data, such systems had to be developed separately.

32. In the UK, the Home Office coordinates and manages investment to ensure that the data retained by CSPs can be accessed by law enforcement organisations effectively and efficiently. As such, the Investigatory Powers Bill additionally includes provision for the request filter specifically to assist with complex communications data investigations. The Bill also allows for CSPs to provide processing that will minimise the amount of data that needs to be processed for the purpose of a disclosure.

33. The Home Office and law enforcement community have developed business change capabilities to support the introduction of new types of communications data including training arrangements for Single Point of Contact (SPoCs) and investigators.

Conclusion

34. The Joint Committee agreed that the provisions for retention of ICRs should be included in the Bill. They will enable law enforcement organisations to continue to protect the public and investigate crime in an increasingly online world.

35. The Home Office has a good track record of working with CSPs to provide operational value for law enforcement through individual retention notices. The Home Office and CSPs are already working together to improve access to IP data by implementing the IP address resolution provisions in the Counter Terrorism and Security Act 2015. This work provides a foundation of joint technical and operational understanding which will underpin the approach to implementation of ICR retention. The Home Office will continue to work closely with CSPs to refine the approach to ICRs in order to ensure that their implementation remains feasible and cost effective. Throughout this process the Home Office will also continue to engage with operational stakeholders to ensure that the proposed implementation will deliver operational value.

36. The experience of Denmark provides important lessons which have been carefully considered in the design of the powers for retention of ICRs included in the Bill and the draft Communications Data Code of Practice. This, together with the UK policy of cost recovery for CSPs, provides the necessary flexibility to tailor the design of ICR retention models to be cost effective and appropriate to individual CSPs, whilst providing the essential framework of controls and oversight to ensure that they are used appropriately.