Internet Society of Australia

A Chapter of the Internet Society

ABN 36 076 406 801
PO Box 1705 North Sydney NSW 2059

6 August 2014

Ten questions about metadata retention

The Australian Government has announced that it will mandate the retention of communications metadata for two years in order to assist law enforcement and national security agencies to improve the detection of terrorism offences and reduce the risk of a terrorist attack within Australia or which affects Australians or their interests.

There has been criticism of this proposal on the grounds of interference with the privacy of the vast majority of Australians who are not terrorists as well as the cost and risks of implementation.

Reassuringly, the Attorney General and Minister for Communications have made it clear that, as a general principle, the Government will seek to minimise the cost impact and risk of interference with the privacy of ordinary Australians to the extent possible.

However, unfortunately at this point there appears to be insufficient information in the public domain about the detail of the proposal to understand how it is to be implemented in practice and to reach informed conclusions as to whether the benefits of the proposal outweigh its cost and risk.

The Government has criticised previous governments for the implementation of major communications projects without adequate consideration, planning and design including a formal business case identifying and weighing the benefits of the project against its costs and risks. It is arguable that this is indeed fair criticism.

Accordingly, the Internet Society of Australia expects the Government to ensure that the design and implementation of the metadata retention proposal is not rushed, chaotic or inadequate, by requiring a rigorous business case and/or regulatory impact assessment process which takes into account the costs and risks of the proposal across industry and the economy as a whole, as well as the direct costs to the Commonwealth budget and risks to the Commonwealth.

We also recommend that the Government conduct a full privacy impact assessment of the proposal in accordance with the Office of the Australian Information Commissioner's guidelines, in addition to any usual parliamentary processes to scrutinise and improve legislation before it is adopted.

Based on the technical and policy experience of its members, the Internet Society of Australia has posed the following questions in relation to the proposal which will require further consideration as part of the various policy, legislation and technical development and assessment processes for the proposal:

1. **What is the definition of metadata to be retained?** If carriers or other organisations are to be obliged to retain metadata, they need to know what metadata is to be retained. The scope of the data required to be retained will have significant impact on the cost and risk in implementing the proposal. Is it

only Internet connection duration and location information, such as that from authentication systems? Is it IP packet headers, or a subset of the information contained in the packet header, or the full content of some of the packets, for example the contents of the packets which include email subject headings? Will information about the content of the packets themselves be required to be retained? Must the metadata of every packet be retained or only session information?

2. **Which entities are required to retain metadata (Retention Entities)?** Will it be restricted to only licensed carriers transmitting information across the public Internet? Will organisations which operate private internal IP networks or virtual private networks be required to retain the metadata of information passing across their private networks, or only if and once the communication leaves the private network to the public Internet?

3. **Whose metadata is required to be retained?** Is it the metadata of all individuals, companies, media organisations, members of parliament, political parties, governments and agencies (including the law enforcement and national security agencies themselves)? Will it apply to the metadata of communications by autonomous devices, like smart meters? If there are to be exceptions, what is the basis for those exceptions and how will the exceptions be implemented in practice?

4. **What method of metadata retention must a Retention Entity employ?** Will it be sufficient for Retention Entities to maintain records in a large range of devices across their networks or will the metadata need to be centralised into a single server or data centre? If so, will the centralisation need to occur in real time (which might considerably increase the network overhead and thus require capacity upgrades across the entire network) or can it be batched and transmitted in periods of lower network traffic? If so, how frequently must it be batched and transmitted? What will be the consequences of failing to do? What format is the metadata required to be collected and stored in? Will the format be standardised or different for different types of communications and storage medium or vendor equipment? What minimum level of security must the Retention Entity establish and maintain in relation to retained metadata? Will a Retention Entity be restrained from outsourcing and/or offshoring the performance of its retention obligations? If not, does the Retention Entity remain primarily liable for those obligations?

5. **When must metadata retention commence?** The Government has indicated that there is an immediate serious risk to the Australian community from terrorism which metadata retention and access will assist to mitigate. Accordingly the Government will seek to implement some form of voluntary informal metadata retention arrangements by direct discussions with the communications industry prior to the introduction of legislation. However, implementation of a metadata retention system is likely to require adequate time to properly plan, design, implement and test before it 'goes live'. Too rapid implementation is likely to:

    5.1 unexpectedly incur or bring forward capital costs which have not been previously budgeted for or funded which may create short term

competitiveness or even liquidity issues, particularly for smaller Retention Entities;

5.2 increase total costs of implementation due to uncertainties in the specification of the form of metadata retention required to be implemented and changing requirements through the various review and parliamentary processes; and

5.3 increase the risk of unidentified defects in design and implementation, thereby increasing the total risk of project failure, loss or disclosure of retained metadata and future requirements to incur additional costs of rectification.

6. **Who will pay the cost of metadata retention?** Will there be some public subsidy to private organisations to meet the capital and operational expenses of implementing and operating metadata retention? Or, will the cost need to be absorbed by customers and/or shareholders? If there is to be some form of public subsidy, on what basis will it be calculated and allocated between Retention Entities? What will the costs of operation of the subsidy system be and how will that be allocated between the public and private sectors? A practical mechanism may be to require relevant law enforcement or national security agencies to subsidise the Retention Entities' capital implementation costs and then pay the true operational cost of each access request they make from their existing budget allocations. This would create a practical budgetary incentive upon agencies to restrict the requirements of (and thus cost of) metadata retention systems and the number of access requests to only the most important and to limit 'fishing expeditions'.

7. **What authorisation will be required to access metadata?** Will metadata be available only to law enforcement (ie Police) and national security agencies? What are the range of agencies permitted to seek access to retained metadata and the purposes for which they may seek access? Will it be limited to intelligence and policing agencies for counter-terrorism purposes or extend to 'ordinary' criminal or civil law enforcement activity. For example, will ASIC, local governments, the Victorian Taxi Directorate and the RSPCA continue to have the ability to access retained metadata for the enforcement of the statutes for which they are responsible, as currently? In what circumstances will a warrant or formal authorisation be required? Will that be an independent process? What oversight will be in place? What sanctions will be applied to individual officers who inappropriately authorise access? What sanctions will apply to agencies and officers who inappropriately use or disclose metadata which has been accessed? Will the Retention Entity be permitted to access its retained metadata for its own business (including billing and marketing) or other purposes? Will private parties to litigation (for example, unfair dismissal, breach of confidence or divorce cases) be able to demand the provision of metadata upon subpoena? Will metadata of, or held by, agencies be available under Freedom of Information requests?

8. **How long must metadata be retained and how will it be disposed of?** Is the two year period foreshadowed by the government the specific, minimum or maximum period for which the data is to be retained? Will agencies be authorised to access metadata which is more than two years old? What

obligations will Retention Entities have to ensure that retained metadata is disposed of and fully expunged after the expiry of the two year period?

9. **Who will bear the risks of metadata retention?** It is likely that any 'deep pool' of metadata will pose an attractive target to hackers, ranging from the purely curious through the disorganised anti-social to organised crime and terrorist organisations themselves. As the Manning and Snowden cases make clear, no information system is ever completely secure, so there is a real probability that retained metadata will be accessed inappropriately or without authorisation, in a way that causes real personal and economic harm. Who bears the costs of that harm: is it the individual whose privacy is interfered with; the business who suffers loss or damage from the disclosure of its confidential information; the Retention Entity which is retaining the data; or the taxpayer through the government? What mechanisms, for example statutory indemnities or immunities, will be put in place to give effect to that risk allocation? What disclosure regimes will be in place in order to report such breaches?

10. **What ongoing review and reporting of metadata retention will occur?** Is the metadata retention intended only to be in place for the next five years, which the Director General of ASIO has identified as the peak risk period for returning jihadists, or will it be in place indefinitely? This will affect the way Retention Entities amortise any of their unsubsidised capital costs of implementing retention systems. Will there be a review of metadata retention? Who will conduct the review, by what process and when? What statistics and key performance indicators of the effectiveness of the proposal in achieving its stated aims will be collected, analysed and published to enable a review to occur?

About the Internet Society

The Internet Society is the world's trusted independent source of leadership for Internet policy, technology standards and future development. Based on its principled vision and substantial technological foundation, the Internet Society works with its members and Chapters around the world to promote the continued evolution and growth of the open Internet through dialogue among companies, governments, and other organisations around the world. See www.internetsociety.org

The **Australian Chapter of the Internet Society** is ISOC-AU, a non-profit society founded in 1996, to promote Internet development in Australia for the whole community and is a peak body organisation, representing the interests of Internet users in Australia. See: www.isoc-au.org.au

Narelle Clark
President

Contact:

Narelle Clark
President
Ph: 0412 297 043
President@isoc-au.org.au

The Internet is for everyone!