Given the alarmingly abbreviated consultation period over the Christmas break, it has been near-impossible to consult with my representative politicians on this matter, and given the closing date of 13-1-17 on the materials i downloaded, I am forced to make a brief comment without the neccessary deeper background research.

1. Contexual

Scheduling this consultation period with this timing and short horizon over a period of universal holiday absences must be regarded as a suspicious action

2 The inability to define the existnig enacted Data Retention scheme in any but the loosest manner, means that the coverage of IoT, Smart meters and almost all devices capable of communication is currently captured. This has already been ruled unconscionable by the EU. No comment about extension of this regime to civil cases can be considered without a clear and properly defined Data Retention set of clear regulations, which can be handled by ISPS without near total data capture including content due to the complexity imposed by the current vague regulations.

3. As Australia still does not have tort of privacy, this regime, extended to any civil domain is unconscionable. For criminal cases there are existing powers, it is for civil cases that the concern has proved to be solid, substantiated, and in developed countries enacted against (vide EU). Even if there was the exemptions for political purposes and small companies make this a limited remedy unless legislated with a much wider scope

4. Any extension at all to Civil Cases undermines the community trust in limitation to national Security issues, where a preventative and probabalistic mode is essential, supported by such measures. However the trust break inevitable by the incremental extension to civil cases means that once again Civil Law and National Security logic is being conflated. This is inappropriate and very dangerous to community trust and is a qualitative change, not a quantitative one. In the absence of a Privacy Tort this makes it almost uncontestable, which is an aspect of inappropriate and unbalanced information power that is already beginning to disturb many member of the community. The lack of transparency is an issue that National Security can sustain, but not when Civil cases are in question.

5. The recent large scale public failures of proper moderation and the lack of practical contestability in both Census and CentreLink has demonstrated to a large

fraction of the population how vulnerable they are to such mass data asymmetries- that are in most cases completely uncontestable for the ordinary person... as so many cases are demonstrating.

6. The lack of any enactment of the Data Breach legislation, with both disclosure and substantial penalties- and consequential damage recompense- is a major failure of the Government's Open Data and eGovernment initiatives as a whole, and this applies *a fortiori* to the proposed extension of access to Data retention to Civil Law. Once the gulf between National Security and Civil law is bridged incremental extension will occur, without doubt

7. The sheer attractiveness of these mass data holding, for data mining, social network establishment and surveillance, and detailed historical and indeed real time micro surveillance are powers that should be reserved solely for National Security. The attempts by RSPCA, local councils etc etc to access the data retention holdings demonstrate the pressure from organisations to secure this level of unbalanced information power over the community at large. It is clear that this is a honeypot for any hackers, both official and unofficial, **locally and globally**

8 At the existing Acts make quite clear, this extension would seem to be most applicable to foreign entertainment companies using it to enforce one sided copyright actions, going beyond the massive speculative trawling John Doe actions that brought them into disrepute even in their home base of the USA.

Recent experience in Australia has shown unequivocally and beyond any further doubt that providing reasonably priced and timely access to copyright entertainment has an immediate a very substantial reduction in 'piracy' (please note the inappropriate use of geoblocking by some streaming suppliers is publicly not supported even by the present Australian government, as people are paying in full but still deemed by foreign parties a 'piracy' and seek to be blocked). These events have brought home to Australian at all levels just how far the entertainment industry overseas is inevitably going exploit any Civil Law access to data retention micro surveillance data.

Comment

Without the safeguards as listed above it is entirely inappropriate to create a civil use exemption as proposed.

The vulnerability of many members of the community to abuse-which will inevitably occur - is a major concern - and the steady incremental of unbalanced population surveillance access is dangerous both to National Security (by conflating the two very different social contracts) and to individuals

This basic worry is well founded, far from alarmist, and has been recognised by most other developed countries, even those with the essential protections of privacy torts and data breach penalties.

The opening to Civil Cases is also vulnerable to regular two yearly access claims to build up log term profiles at a micro level - very attractive to a range of civil organisations and government instrumentalities. No constraints on this predictable action have even been hinted at in any draft legislation or public consultation proposals.

Conclusion

This proposal is premature, and should only be even considered after penal Data Breach and Privacy tort legislation has been fully enacted and been in place, and far greater transparency is also required if any Civil Cases are to be given any access to this extremely powerful population surveillance database.

Prior to that, substantial refinement of the existing opaque Data Capture and Retention initiative is a sine qua non

Submitted by Dr Marcus R Wigan

Professor Emeritus Edinburgh Napier University