MACQUARIE University
SYDNEY·AUSTRALIA

Communications Security Branch
Attorney-General's Department
3-5 National Circuit
BARTON ACT 2600

email: CommunicationsSecurity@ag.gov.au

27 January 2017

Dear Attorney-General's Department and Department of Communications & the Arts,

Re: Submission to the Retained Data in Civil Proceedings Consultation

Please find attached my submission to the consultation on retained data in civil proceedings. You may publish it with my name attached.

Regards,

J. Selby

Dr John Selby

Faculty of Business & Economics

Macquarie University

Email: john.selby@mq.edu.au

MACQUARIE University
SYDNEY·AUSTRALIA

27 January 2017

Dear Attorney-General's Department and Department of Communications & the Arts,

Re: Consultation on Proposed Expansion of Access by Civil Litigants to Retained Metadata

Introduction

Thank you for the opportunity to participate in this consultation on the proposal to expand access by civil litigants to retained metadata. This submission builds upon my previous submission to the 2015 Parliamentary Joint Committee on Intelligence and Security's Inquiry into Retained Metadata.[1]

For operational purposes telecommunications service providers have historically kept only limited types of metadata for limited amounts of time. Whilst a civil litigant can seek a court order for a subpoena to be served upon a telecommunications provider so as to compel them to disclose historical records for the purposes of civil litigation, those records cannot be disclosed by the telecommunications service provider in compliance with the subpoena if the telecommunications service provider either:

a) never collected that type of metadata at any time;

b) collected that type of metadata at the relevant time, but destroyed its records of that type of metadata prior to the date of receiving the subpoena.

Extension of the Retained Metadata Law beyond terrorism and serious criminal cases would alter the volume and types of information capable of being subpoenaed by civil litigants by changing both a) and b) above. The consequences of this proposed change are significant, and may dramatically affect the conduct on political, business and social affairs in this country. As such, expansion of access to retained metadata to civil litigants should not be undertaken.

[1] Submission 114: <http://www.aph.gov.au/DocumentStore.ashx?id=e20a8e96-f97f-4d73-adb4-80e935516084&subId=302752>

Part 1 of this submission addresses two systemic flaws with this proposal:

a) civil litigants are not under the same restrictions as the government to act as model litigants;

b) metadata accessed through civil litigation could be used as a strategic tool to achieve a variety of nefarious objectives, which could undermine public support for this policy.

Part 2 of this submission provides partial answers to the three questions asked in the consultation paper.[2]

Part One:

There is a significant difference between the role/behaviour expected of the government in criminal litigation / intelligence enforcement and the role/behaviour expected of private civil litigants

There is a significant difference between access and use of retained metadata by the Commonwealth as plaintiff in criminal law / by government intelligence agencies as part of their counter-terrorism intelligence efforts, and access and use of retained metadata by civil litigants.

When bringing or defending a matter in court, the Federal government is constrained by the requirement that it act as a "model litigant".[3] Whilst the Federal Court Rules[4] and Uniform Civil Procedure Rules[5] impose restrictions on how civil litigants can conduct their matters in court, those restrictions are not as onerous as those imposed upon the Federal Government.[6] Notably, whilst lawyers may face personal cost penalties for bringing such

[2] Given the limited time to prepare a response (and timing) of this consultation, it has not been possible to prepare a thorough analysis of all of the civil litigation issues potentially relevant.
[3] s55ZF *Judiciary Act* 1903 (Cth) and Appendix B of the *Legal Services Directions* 2005 (vF2016C00965): <https://www.legislation.gov.au/Details/F2016C00965>
[4] See, for example, the process for striking out vexatious proceedings under s37AO of the Federal Court of Australia Act 1976 (Cth)
[5] See, for example, s2(1) of Schedule 2 of the *Legal Profession Uniform Law Application Act* 2014 (NSW) which requires legal practitioners to certify that a dispute has a reasonable prospect of success prior to lodging the statement of claim.
[6] "However, it is clear that some of the obligations imposed under the Model Litigant Policy go beyond those imposed on private litigants": Eugene Wheelahan, 'Model Litigant Obligations: What Are They and How Are They Enforced' *Presentation to the Federal Court Ethics Series* (15 March 2016) <http://www.fedcourt.gov.au/__data/assets/rtf_file/0011/31142/20160315-Eugene-Wheelahan.rtf>.

actions to court[7], a self-represented civil litigant may bring an action without having to certify that it has a "reasonable prospect of success".[8]

There are several ways in which retained metadata in civil litigation could be mis-used by individuals, organisations or corporations, including:

a. Prospects for Abuse #1: Civil Litigation as a back-door method to gain access to valuable metadata for nefarious purposes (crimes such as insider trading) or to achieve inappropriate benefits (influencing settlement and custody dispute in divorce proceedings)

My earlier submission to the PJCIS Inquiry raised the risk of retained metadata held by telecommunications service providers being accessed by criminals for the purposes of committing crimes such as insider trading.[9] The PJCIS recognised this risk and recommended that telecommunications service providers increase the security they placed around their retained metadata.[10]

The proposal to allow civil litigants to gain access to retained metadata risks undermining those efforts to increase the security of retained metadata. Motivated criminals would not need to hack into the secured retained metadata database held by a telecommunications service provider so as to gain information necessary to engage in insider trading. Instead, they could use a front person to lodge a (trumped-up) lawsuit against a targeted person and use the court's subpoena powers to gain access to that targeted person's metadata. The applicant could then surreptitiously share the retained metadata with criminals, who could then undertake insider trading on the basis of that information. The targeted person would risk the expense of having to challenge un-meritorious civil claims being made against them without necessarily realising the underlying criminal purpose of those claims.

---

[7] The trial judge in *Ashby v Slipper* made adverse findings against Ashby's lawyer for bringing an action without reasonable prospects of success. Those findings were overturned on appeal. In the USA, there have been cases where lawyers have abused the legal system to lodge cases with phantom defendants: see <https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/10/10/dozens-of-suspicious-court-cases-with-missing-defendants-aim-at-getting-web-pages-taken-down-or-deindexed/?utm_term=.45a23528a8da>

[8] For judicial consideration of "no reasonable prospects of success", see: *Boston Commercial Services Pty Ltd v GE Capital Finance Australasia Pty Ltd* [2006] FCA 1352; *Dura (Australia) Constructions Pty Ltd v Hue Boutique Living Pty Ltd No.5* [2014] VSC 400; *Ashby v Slipper* [2014] FCAFC 15; *Queensland University of Technology v Project Constructions (Australia) Pty Ltd (in Liq) and Anor* [2002] QCA 224, and cases cited therein.

[9] Whilst this might seem a fanciful prospect, similar insider-trading attacks have already occurred in the real world. The US has already seen a spate of attacks upon advisory firms such as lawyers and investment bankers by foreign cybercriminals motivated to engage in insider trading. See, for example, the Indictment against Iat Hong, Bo Zheng and Chin Hung dated 13 October 2016 from the US District Court, Southern District of New York <https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-arrest-macau-resident-and-unsealing-charges-against>. Those defendants were alleged to have "carried out a scheme to enrich themselves by obtaining and trading on material, non-public information exfiltrated from the networks and servers of the victim law firms concerning M&A transactions", earning $US 4 million between 2014 and 2016.

[10] Parliamentary Joint Committee on Intelligence and Security, *Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, (2015), [5.60] and [5.67]

b. Prospects for Abuse #2: Civil litigation against politicians or other persons of public interest for the purposes of gaining access to their metadata

As seen in the lengthy litigation undertaken by James Ashby against Peter Slipper MP[11], civil actions against sitting politicians are not unheard of. Such civil litigation can be extremely damaging to the career of a politician or other person of public interest, even if they (the politician or other person of public interest) ultimately prevail in the courts.[12] Giving civil litigants the ability to gain access to the retained metadata of politicians and other persons of public interest may result in an increase in the number of un-meritorious civil lawsuits lodged against them by persons, organisations or companies motivated to smear them or to weaken their likelihood of continued success in their careers. Such metadata could include the politician's or person of public interest's location (mobile phone data)[13], to whom they have sent/received SMSes[14], and/or the subject-line and to whom they have sent/received emails.[15]

As discussed above, individuals, organisations and companies are not subject to as stringent requirements regarding their conduct of civil litigation as the Commonwealth, so the potential for abuse is significant.

c. Prospects for Abuse #3: Lawsuits targeting persons who challenge the status quo, such as by employers against vulnerable employees and/or whistle-blowers

In a democracy such as Australia, it is the right of citizens to be able to peacefully challenge the status quo in society. Giving civil litigants access to up to two years of retained metadata may discourage such valuable public debate because persons who seek to challenge the status quo may feel less likely to engage in such valuable public debates due to the risk of being subject to civil litigation designed to gain access to their personal metadata. For example, giving employers the ability to access up to two years of retained metadata

---

[11] See, for example, *Ashby v Slipper* [2014] FCAFC 15 <http://www.austlii.edu.au/cgi-bin/sinodisp/au/cases/cth/FCAFC/2014/15.html>

[12] Ashby abandoned his action against Slipper in 2016 and was later the subject of an Australian Federal Police Inquiry into whether his unauthorised conduct in disclosing Slipper's diary may have been criminal.

[13] For example, in 2017 Federal Health Minister Sussan Ley recently resigned over an expense claims scandal, including those expenses relating to travel to the Gold Coast to purchase an investment property <http://www.abc.net.au/news/2017-01-13/sussan-ley-tenders-resignation-parliament-expenses-scandal/8180602>. A civil litigant who had access to Minister Ley's metadata could potentially have determined from her mobile phone cell-tower metadata precisely where she had been (and for how long) on each taxpayer-funded trip for the past two years.

[14] For example, in 2007 the Victorian state parliament Liberal MP Richard Dalla-Riva resigned after it was revealed that he had sent harassing text messages to an 18-yo woman at a party function the previous year: <http://www.abc.net.au/pm/content/2007/s1840903.htm>.

[15] For example, in 2014, Federal Labor Senator Nova Peris was involved in a scandal regarding whether she had sent emails to a lover whom she was allegedly seeking to secure government funding for a visit to Australia: <http://www.smh.com.au/federal-politics/political-news/media-went-too-far-on-nova-peris-email-scandal-says-malcolm-turnbull-20141030-11ennw.html>.

relating to their employees creates the potential for an expansion of workplace and personal surveillance of employees in ways which would not otherwise be acceptable to the Australian public. Employers could use this information to target union organisers, whistleblowers, or simply to find justifications to sack unpopular or inconvenient staff. The mere possibility of being able to gain access to such metadata through civil litigation could be used by employers as a tool to oppress employees.

Part Two:

Q1. In what circumstances do parties to civil proceedings currently request access to telecommunications data in the data set outlined in section 187AA of the TIA Act (refer to Attachment A)?

Response:
Plaintiffs in civil litigation who do not know the identity of the defendant they wish to sue can apply to the court for an order for preliminary discovery.[16] In making such an application, the plaintiff provides to the court whatever information that they have about the potential defendant (which might be, for example, an email address, telephone number or IP address) and the details of third parties (such as an email provider like Google for Gmail addresses, or Microsoft for Hotmail addresses, an ISP like Telstra for IP addresses, or a telecommunications service provider like Optus for phone numbers) who might be able to connect that metadata to the personal identity of that provider's customers. The applicant also provides a description of the unsuccessful attempts that the applicant has made to find the identity of the defendant (for example, by sending an email to the email address, calling the telephone number, etc.).

If the court grants the order for preliminary discovery, the plaintiff provides that order to the third party and requests them to provide the relevant customer information, or to attend court to answer questions as to who is their customer. These orders might need to be sought multiple times in an iterative fashion as the plaintiff tries to unmask the identity of the defendant. For example, an email provider can give information about the IP addresses used to create the account and send emails, which might then lead to the plaintiff making further preliminary discovery orders against the ISP to whom has been issued the range of IP addresses into which that particular IP address falls. The ISP may then be able to identify to which of its subscribers it had issued that dynamic IP address at the relevant date and time. The plaintiff may then seek a third preliminary discovery order to compel the subscriber to answer questions about the identity of the person or persons it had permitted to access the Internet via its network or computers at the relevant time.

The difference between access by civil litigants to retained metadata and existing access through preliminary discovery orders is the extent and period of time for which a person's personal information can be accessed by plaintiffs. Preliminary discovery orders are usually granted only in relation to specific metadata for specific dates and times (e.g. which

[16] See, for example, Part 5 of the *Uniform Civil Procedure Rules 2005* (NSW): <http://www.austlii.edu.au/au/legis/nsw/consol_reg/ucpr2005305/>

subscriber sent an email from this email account using this IP address at this time on this date?). Access to retained metadata for broader civil litigation purposes might enable a plaintiff to gain access to reconstruct the life habits and movements of a defendant for up to two years.

Q2. What, if any, impact would there be on civil proceedings if parties were unable to access the telecommunications data set as outlined in section 187AA of the TIA Act?

Response:
Using the preliminary discovery process, civil litigants can already access a subset of the telecommunication data set as outlined in s187AA of the TIA Act. If they have been too slow to bring their action before the courts, some civil litigants might not be able to identify defendants using the preliminary discovery application process discussed in my answer to Q1 because the telecommunications service provider may have either not collected that data or ceased to retain it because it was not needed for business purposes.

If the limitation precluding the use of retained metadata in civil litigation is enforced, parties to litigation would not be able to use two years of retained metadata to reconstruct the life habits and movements of a person (most likely the defendant) for up to two years.

Q3. Are there particular kinds of civil proceedings or circumstances in which the prohibition in section 280(1B) of the *Telecommunications Act 1997* should not apply?

Response:

Simply put: No.

The examples of "violence or international child abduction cases" presented in the consultation paper should be prosecuted as serious crimes (e.g. battery / kidnapping) rather than civil proceedings. As such, those examples already fall within the ambit of the exemption for terrorism/serious crimes that formed the original justification for this legislation.

Yours sincerely,

J. Selby

Dr John Selby
Faculty of Business & Economics
Macquarie University
Email: john.selby@mq.edu.au