Submission No 110

Inquiry into potential reforms of National Security Legislation

Organisation: Mr Daniel Nazer

Daniel Nazer

Residential Fellow at the Center for Internet and Society

Stanford Law School

submission to

Inquiry into Potential Reforms of National Security Legislation,

Parliamentary Joint Committee on Information and Security

Introduction and Summary

1. I am an Australian citizen currently employed as a Residential Fellow at the Center for Internet and Society (CIS) at Stanford Law School. CIS is a public interest technology law and policy program that brings together academics, students, programmers, security researchers, and others to study the interaction of new technologies and the law, with a particular focus on technology's impact on public goods like free speech, innovation, and privacy. I make this submission in my personal capacity.

2. I make the following recommendations:

   a. ***The Committee should reject the Government's proposal to implement data retention***.

   b. ***The Committee should reject the Government's proposal to expand the ASIO Act's warrant deadlines.***

   c. ***The Committee should maintain the TIA Act's existing record-keeping requirements and accountability measures for warrants.***

Data Retention

Defining data retention

3. The Government has asked for the Committee's views regarding "tailored data retention periods for up to 2 years for parts of a data set, with specific timeframes taking into account agency priorities, and privacy and cost impacts." At the outset, it is essential to define 'data retention.' Under a data retention regime, telecommunications providers, including internet service providers (ISPs), are required to log and retain certain kinds of communications data for *all* of their users so that law enforcement agencies can later access the data if requested. This data is retained whether or not the service provider has a business need to store the data. Similarly, the data is retained even though there is no basis to suspect the users of wrongdoing.

4. The precise contours of a data retention regime can vary widely. A data retention program must consider: (1) which service providers will be required to retain data; (2) what categories of data must be retained; (3) how long the data must be retained; (4) who may gain access to the data; and (5) the procedures and safeguards governing access to the data. The Attorney-General's discussion paper offers a clear proposal regarding only

one these five key issues (proposing a retention period of two years). Other key issues include whether the program will require retention of browsing history revealing all websites visited by any Australian.

5. Data retention should be contrasted with data preservation. A data retention program affects all users. In contrast, a data preservation approach allows the Government to require that an individual suspect's data be retained for a certain period of time pending a warrant or court order granting access to the data.

The Attorney-General's Department has failed to provide a detailed data retention proposal or any cost-benefit analysis

6. This is not the first time that a parliamentary committee has considered data retention. The Senate Environment and Communications Reference Committee (the SECRC) recently held an inquiry, and issued a report, regarding the adequacy of protections for the privacy of Australians online.[1] A number of submissions to that inquiry commented on data retention and the topic was also discussed during hearings.[2] The SECRC concluded that data retention has "very serious privacy implications" and that there is a real possibility that it is "unnecessary, will not provide significant benefit to law enforcement agencies, and is disproportionate to the end sought to be achieved."[3]

7. The SECRC criticised the Attorney-General's Department's "narrow consultations" on the issue, finding that the Department had consulted with business interests but had not consulted "with the broader community or public interest and civil liberties organisations."[4] The SECRC expressed concern that the Government had not provided meaningful details of its proposal.

8. The SECRC recommended that, before the Government pursue any mandatory data retention program, it must:

    - undertake an extensive analysis of the costs, benefits and risks of such a scheme;

[1] Senate Environment and Communications References Committee, Parliament of Australia, *The adequacy of protections for the privacy of Australian's online* (2011) (hereafter 'SECRC Report').

[2] *See ibid*. at [4.1 - 4.75].

[3] *Idid.* at [4.70].

[4] *Ibid.* at [4.70].

- justify the collection and retention of personal data by demonstrating the necessity of that data to law enforcement activities;
- quantify and justify the expense to Internet Service Providers of data collection and storage by demonstrating the utility of the data retained to law enforcement;
- assure Australians that data retained under any such scheme will be subject to appropriate accountability and monitoring mechanisms, and will be stored securely; and
- consult with a range of stakeholders.[5]

9. The Attorney-General's Department has not addressed the concerns of the SECRC. Instead, it has returned to Parliament with another vague and poorly justified proposal. It has not conducted an extensive cost-benefit analysis and has not provided evidence showing that preserved data will be stored securely. The Department has also failed to provide important details (for example, the discussion paper does not specify the categories of data the Government proposes should be retained).[6] Without such details, the public, and the Committee, is left to guess what the contours of an Australian data preservation regime might be.

10. Before considering data retention, this Committee should require the Attorney-General's Department to address all concerns raised by the SECRC. At a minimum, the Department should conduct broad consultations, provide a concrete proposal, and undertake a cost-benefit analysis.

11. In the remainder of these comments, I will assume that the Department is proposing a data retention plan similar to Directive 2006/24/EC of the European Parliament, which requires that providers of fixed network telephony, mobile telephony, and internet services are obliged to retain traffic and location data of users for up to two years.[7]

---

[5] *Ibid* at [4.74]

[6] As of 1 December 2010, the Attorney-General's Department stated that it had "developed a 'data set' of the categories of information to be retained." *Ibid.* at [4.34] (testimony of Ms Catherine Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch, Attorney-General's Department). The Department did not include these categories in its discussion paper, however.

[7] Note that the EU Directive has been found unconstitutional by national courts in both Romania and Germany. *See* Federal Constitutional Court of Germany, Press release no. 11/2010 (2 March 2010), <http://www.bverfg.de/pressemitteilungen/bvg10-011en.html>; Romanian Constitutional Court, Decision no.1258, 8 October 2009, http://www.legiinternet.ro/english/jurisprudenta-it-romania/decizii-it/romanian-constitutional-court-decision-regarding-dataretention.html.

Data retention harms both privacy and security

12. Australians use the internet for a wide range of highly sensitive personal communications. These can range from emails between family members, reading online books, or consulting with health care providers.[8] A data retention regime would require private companies, acting on behalf of the Government, to collect and store every one of these communications. Such widespread surveillance raises serious privacy concerns.

13. Firstly, the creation of large databases of customer communications harms both privacy and security by making huge amounts of data available for potential misuse. It also creates an attractive target for hackers. Privacy experts have long recognised that data minimisation is an essential tool for effective privacy protection. As Dr. Ann Cavoukian, Information and Privacy Commissioner of Ontario, Canada, has explained:

> Data minimization is essential to effective privacy protection, and can save organizations the risk and expense of managing personal information they may have no need for. Where there is no personal information, there is no consequent duty of care, with all that it implies. Further, data minimization requirements assists organizations to think through what personal information is actually necessary for their purposes, and guards against secondary uses and possible function creep.[9]

14. Mandatory data retention flatly contradicts the principle of data minimisation. Instead, it forces service providers to store enormous amounts of data for which they have no business need. This creates the risk of inadvertent disclosure, misuse, or breach.

15. The danger of breach by outsiders is very real. In the United States, for example, the Privacy Rights Clearinghouse has compiled evidence of

---

[8] *See, e.g.*, Centre for Mental Health Research, Australian National University, *e-Mental Health in Australia: Implications of the Internet and Related Technologies for Policy* at 69 (noting that the internet will play a major role in the "delivery of programs aimed at increasing community awareness and in providing prevention, assessment, diagnosis, counselling and treatment programs.").

[9] Dr. Ann Cavoukian, Ph.D., Information and Privacy Commissioner of Ontario, Canada, *Submission to Consultation on the European Commission's Comprehensive Approach on Personal Data Protection in the European Union* (2011), available at <http://ec.europa.eu/justice/news/consulting_public/0006/contributions/public_authorities/ipc_info_and_privacy_comm_ca_en.pdf>

thousands of data breaches involving more than half a billion records.[10] Numerous security breaches have also been recorded in Australia.[11] Furthermore, since Australia does not a mandatory data-breach reporting law, it is likely that many addition breaches in Australia are unreported.[12] If all Australian's communications are stored, a security breach will expose data from hundreds of thousands, or even millions, of customers at once. Thus, while there is only very small probability that a particular user's retained data will ever be useful to law enforcement, there is a much larger probability that the user's data will be the subject of a security breach.

16. Data retention also creates a risk of function creep by the service providers. If the Government forces companies to spend money building expensive customer databases then businesses will be tempted to find commercial uses for that data (such as selling the information to telemarketers or spammers).[13]

17. The Attorney-General's Department might produce a plan that purports to exclude data revealing the content of communications.[14] In practice, however, ISPs cannot or do not separate purely transactional data from that which reveals content. For example, a log of IP address a user visits reveals what the user read and other contents of the user's browsing history.[15] In telephone transactions, the phone numbers dialled may not be content, but numbers input after connection in response to a phone tree or other verbal prompts, called post cut through dialled digits (PCTDD), are

[10] Privacy Rights Clearinghouse, *Chronology of Data Breaches, Security Breaches 2005 – Present* (updated August 5, 2012), available at <http://www.privacyrights.org/data-breach> (listing 3,273 data breaches, involving 563,219,356 records, made public since 2005).

[11] Office of the Australian Information Commissioner, *Media Release: Business warned to be ready for data breaches* (April 30, 2012), available at <http://www.oaic.gov.au/news/media_releases/media_release_120430_business-warned-to-be-ready.html>; *see also* Craig Scroggie, *Data breaches cost Australian organisations over two million dollars per incident* (April 12, 2012), ABC Technology and Games, available at <http://www.abc.net.au/technology/articles/2012/04/26/3489569.htm>

[12] *See* Michael Lee, ZDNet, *Australia pressured on data breach laws* (July 18, 2011), available at <http://www.zdnet.com/australia-pressured-on-data-breach-laws-1339318719/> ("Even though data breaches have received attention . . . experts believe that those we know about might only be the icing on the cake.").

[13] Telstra was recently discovered to have sent customer browsing history to a third party in Canada to help that company develop censorship systems. *See* Stilgherrian, crikey, *'It's how we connect': Telstra and the spy sites mystery* (June 27, 2012), available at <http://www.crikey.com.au/2012/06/27/its-how-we-connect-telstra-and-the-spy-sites-mystery/>

[14] The Department defines 'data' as "information about a communication that is not the content or substance of a communication." Discussion Paper at 58.

[15] *See* SECRC Report at [4.53] (testimony of Testimony of Ms Miller, Law Institute of Victoria).

content. This content can be highly sensitive, including bank account numbers and PINs for example. We have also seen in Europe that the difficulty in segregating content from non content leads to over-retention. For example, email subject lines may be retained along with other header information, but they are clearly contents of communications.[16]

18. Moreover, because ISPs collect so much data on each user (logging every email, chat, browsing session, and VoIP call), the aggregate of this data will reveal highly intimate details of a person's life, perhaps far beyond what any single message or web session might.[17] Religious and political affiliations are revealed. In fact, large stores like Target can analyse in-store shopping histories to determine when a woman is pregnant, even if she does not want the store to know, so that the retailer can send her early advertisements for prenatal vitamins and baby supplies.[18] In sum, highly personal information can be discovered in vast data sets and exploited.

Data retention imposes costs on consumers and harms competition

19. A data retention regime requires communications providers to store data that they would not otherwise keep. In addition to storing the data, companies must adequately protect its security. These costs will ultimately be borne by the public, whether in terms of higher prices or, to the extent the Government shares the cost, through the tax system. The Attorney-General's Department's discussion paper does not provide any estimate of the economic cost of data retention.

20. The costs of data preservation are likely to fall hardest on smaller companies. Smaller providers may not yet have the infrastructure to store the additional data. Large scale data storage requires expensive hardware,

---

[16] *See* European Union, Article 29 Data Protection Working Party, *Report 01/2010 on the second joint enforcement action: Compliance at national level of Telecom Providers and ISPs with the obligations required from national traffic data retention legislation* 9 (2010), available at <ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp172_en.pdf>

[17] *See* Daniel J. Solove, 'A Taxonomy of Privacy' (2006) 154 *University of Pennsylvania Law Review* 477, 507 ("A piece of information here or there is not very telling. But when combined together, bits and pieces of data begin to form a portrait of a person."). Indeed, because patterns found in databases are so revealing, even anonymised data is often traceable back to individual users. *See* Nate Anderson, *"Anonymized" data really isn't—and here's why not*, arstechnica, available at <http://arstechnica.com/tech-policy/2009/09/your-secrets-live-online-in-databases-of-ruin/>

[18] Charles Duhigg, *How Companies Learn Your Secrets*, New York Times, February 16, 2012 available at <http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?_r=1>

software, and data security expertise.[19] This burden would be especially devastating to online service providers (such as social networking sites) that would not otherwise track the source data of communications. Moreover, many such companies are small start-ups and compete against companies from all over the world. Ultimately, the burden of data preservation could drive smaller communications companies out of business and send innovation overseas.

Narrowly targeted data preservation provides a better alternative

21. To the extent the Government is concerned that data needed for law enforcement investigations is being lost before agencies can secure a search warrant, it should follow Canada's lead and pursue data preservation.[20] This would create a process whereby an agency can secure a temporary preservation order that remains in effect only for as long as it takes law enforcement to return with a warrant. While any data preservation program would still require safeguards to protect privacy, it is certain to be less invasive and costly than massive and indiscriminate data retention.

22. Ultimately, data retention undermines basic privacy. Instead of minimising the collection of personal information, it creates vast databases of every citizen's online activities. In doing so, it treats all Australians as criminal suspects worthy of surveillance.[21] The Committee should reject the proposal.

Warrant duration under the ASIO Act

23. The Attorney-General's Department recommends that the Australian Security Intelligence Organisation Act 1979 (the ASIO Act) be amended to extend the duration of search warrants from 90 days to 180 days. The Committee should reject this proposal.

---

[19] *See generally* Symantec 2010 Information Management Health Check, Global Results (2010) <http://www.symantec.com/content/en/us/about/media/pdfs/symantec_2010_information_management_health_check_report_global.pdf>

[20] *See* Department of Justice, Canada, *Backgrounder: Investigative Powers for the 21st Century Act*, Nov. 2010, available at http://www.justice.gc.ca/eng/news-nouv/nr-cp/2010/doc_32567.html (proposing data preservation and rejecting the idea of widespread data retention).

[21] By subjecting every citizen to surveillance, data retention is in conflict with Article 12 of the Universal Declaration of Human Rights, which prohibits "arbitrary interference" with "privacy, family, home or correspondence." Universal Declaration of Human Rights, Paris, UN GA Res. 217 A (III) of 10 December 1948, art. 12; *see also* Patrick Breyer, "Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR", *European Law Journal*, Vol. 11, No. 3, May 2005.

24. The ASIO Act already provides for search warrants of very long duration. The current 90 day period can be contrasted with Commonwealth warrants issued pursuant to subsection 3E(5A) of the Crimes Act 1914 which are valid for only seven days.[22] Short deadlines for executing a warrant make sense. As days, weeks, or even months go by, it becomes increasingly likely that a search warrant is based on stale information. Indeed, with a deadline as long as 180 days, it is possible that an investigation might evolve to the point of exonerating a target. Thus, limited warrant durations promote privacy by ensuring that searches are conducted based on fresh, accurate information.

25. The discussion paper suggests that there have been instances where ASIO was unable to execute a search warrant within 90 days.[23] ASIO Act subsection 25(11) already makes it clear that ASIO can apply for a "further warrant" after the expiration of that time period. Thus, in such cases, ASIO can simply reapply for a warrant. If the circumstances justifying the warrant have not changed then this is not a significant administrative burden (as ASIO can submit essentially the same information). This occasional and very limited administrative burden does not justify extending the ASIO Act's 90 day deadline for executing search warrants.

Record-keeping requirements

26. The Telecommunications (Interceptions and Access) Act 1979 (the TIA Act) contains a number of safeguards and accountability mechanisms. These include record-keeping requirements found in sections 14, 15 and 17 of the Act, which require reporting agencies to keep records showing how intercepted information is used, disclosed, or destroyed. The Attorney-General's Department's discussion paper suggests removing these record-keeping rules and replacing them with some vague and unspecified "less process oriented" requirements. The Committee should reject this proposal and maintain existing safeguards.

27. Overseas experience confirms the importance of record-keeping and strong public oversight to ensure that covert powers are not abused. For example,

[22] Similarly, federal search warrants in the United States are generally limited to 14 days. *See* United States Federal Rule of Criminal Procedure 41(e)(2)(A)(i). The Foreign Intelligence Surveillance Act of the United States generally provides for warrants of 90 days duration. *See* 50 USC § 1824(d). It provides for a warrant of longer duration only in the limited situation where the target of the warrant is an "an agent of a foreign power who is not a United States person." *Ibid.* If the Committee does recommend any extension of warrant durations, it should similarly limit the extension to serious cases involving agents of a "foreign power" as defined in section 4 of the ASIO Act.

[23] Discussion Paper at 42.

the Inspector General of the United States Department of Justice recently found that the Federal Bureau of Investigation had used covert National Security Letters to make thousands of improper record requests.[24] These problems were far from a few isolated instances. It appears that from 2001 to 2008, the FBI committed as many as 40,000 violations of law, Executive Order, or other regulations governing intelligence investigations.[25] As corrective action, the Inspector General recommended that the FBI implement record-keeping policies very similar to those that the Attorney-General's Department suggests Australia should now abandon.[26]

28. The discussion paper suggests that current record-keeping requirements should be modified because they "reflect historical concerns about corruption and the misuse of covert powers."[27] The Department's argument seems to be: oversight mechanisms have been successful, therefore we should jettison them. This is not persuasive. Moreover, the concern about misuse of covert powers is not 'historical' – it is essential to any open democracy.

29. The Attorney-General's Department has not provided compelling reasons for diluting existing safeguards. History demonstrates that such safeguards are essential in a democracy. Indeed, given that the Government is asking for expanded powers, effective oversight is more important than ever.

I thank the Committee for the opportunity to make these submissions.

For further information contact:
Daniel Nazer
Residential Fellow, Center for Internet and Society
Stanford Law School
559 Nathan Abbott Way
Stanford, CA 94305
U.S.A.
Ph: (650) 325 780
E-mail: dnazer@stanford.edu

[24] Office of the Inspector General, U.S. Department of Justice, *A Review of the FBI's Use of National Security Letters: Assessment of Corrective Actions and Examination of NSL Usage in 2006* (2008), available at <http://www.justice.gov/oig/special/s0803b/final.pdf>.

[25] *See* Electronic Frontier Foundation, *Patterns of Misconduct: FBI Intelligence Violations from 2001 – 2008* (2011), available at <https://www.eff.org/pages/patterns-misconduct-fbi-intelligence-violations>

[26] *See* OIG, *Review of the FBI's Use of National Security Letters*, *supra* note 23, at 14-33.

[27] Discussion Paper at 26.