Digital Rights Watch

Submission to Attorney General's Department consultation:

Access to telecommunications data in civil proceedings

25 January 2017

Who is Digital Rights Watch?

Digital Rights Watch (DRW) is an Australian non-profit charity that supports, fosters, promotes and highlights the work of Australians standing up for their digital rights. http://digitalrightswatch.org.au

Digital Rights Watch recognises and thanks the work of Dr Kylie Pappalardo of Queensland University of Technology Faculty of Law in preparing this submission.

For more information about this submission please contact Elizabeth O'Shea, Board Member of Digital Rights Watch - lizzie@digitalrightswatch.org.au

The context of the data retention regime

The current data retention regime is highly invasive of the privacy of Australian citizens, and a breach of international human rights obligations including the right to privacy. United Nations Special Rapporteur Ben Emmerson recently stated that mandatory data retention 'amounts to a systematic interference with the right to respect for the privacy of communications,' and as such, 'bulk access technology is indiscriminately corrosive of online privacy and impinges on the very essence of the right to privacy.'[1] Opposition to the current Australian data retention regime is a central policy position of Digital Rights Watch.

It is important to note that the core justification made for the data retention scheme at the time it was being debated in Parliament was as a necessity for dealing with serious crimes. The undermining of personal privacy was therefore mandated by an inherent link to prosecuting serious crimes, and was the only justification for the scheme when the legislation was passed with bipartisan support.[2] The broad prohibition on the disclosure of data retained for the purposes of regime in section 280 of the *Telecommunications Act 1997* (Cth) (the **Act**) as amended was essential to the Act's passage.

Digital Rights Watch urges the Australian Government to not abuse the trust of the Australian people by substantially lessening these protections through regulation. The unfettered power to prescribe exceptions to section 280 of the Act, set to commence in April 2017, is an unacceptable watering down of that prohibition. On the fundamental principle that lawmaking should be subject to the full rigours of the parliamentary process wherever possible, we are generally concerned wherever we find broad declaratory powers (such as this) handed to the executive.

It is also important that any discussion about proposed regulatory changes is fully informed. In that context, Digital Rights Watch notes that data retained under the regime can be accessed by law enforcement agencies already in relation to **any** offences, not just serious crimes. The determinative factor in these cases is the agency or applicant, with no threshold in relation to the gravity of alleged conduct in order for prescribed enforcement agencies to access data. The only limit on accessing data retained under the regime is by agency (using a prescribed list) but this list can be added to at any time. Already there are reports of agencies lobbying to get themselves added to the list.[3] It is not clear to Digital Rights Watch how many applications have been made for data and for which offences such applications have been made. This is relevant information for assessing the privacy implications of this evolving field of technology.

---

[1] Online mass-surveillance: "Protect right to privacy even when countering terrorism" – UN expert, 23 October 2014 http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=15200&LangID=E#sthash.YMVF9Bq7.dpuf

[2] See Suzor, N., Pappalardo, K., McIntosh, N. (forthcoming 2017). The passage of Australia's data retention regime: national security, human rights, and media scrutiny. *Internet Policy Review*.

[3] http://www.gizmodo.com.au/2016/01/heres-every-government-agency-that-wants-your-metadata/

As a civil society organisation with a focus on protecting digital rights, Digital Rights Watch is not in a position to answer question 1 as set out in the consultation paper from experience. However, we do note that prior to the introduction of the regime, a range of entities were accessing data for all sorts of legal purposes, including local councils and the RSPCA.[4] It is therefore reasonable to assume that it is likely the prescribed agencies are accessing data retained under the regime for a range of offences, not just those that are serious, or if this is not the case, it will very soon be the practice.

It is reasonable, given the mandate for the original legislation and the community expectations in respect of this issue, that any access to data retained under the regime granted to prescribed agencies be for the purpose of investigating and prosecuting serious crimes only. The government should consider acting on this expectation by enacting a legislative amendment or including such a threshold in any future regulatory drafting. For present purposes, to the extent that any further access to data retained under the regime is being considered for parties outside the prescribed list of agencies, it is vital that there be a threshold level of seriousness of the civil proceedings that must be met before access to is granted.

Digital Rights Watch recommends that the government introduce a legislative or regulatory threshold in relation to the seriousness of the alleged conduct that must be met in order to make an application to access data retained for the purposes of this scheme.

The impact on civil proceedings of a prohibition on accessing metadata under section 187AA

It is Digital Rights Watch's submission that a prohibition on accessing data retained solely for the purpose of complying with the regime would not have an impact on civil proceedings significant enough to justify the invasion of privacy that would result from exceptions.

As a preliminary matter to discussing this issue, it is important to note that the prohibition on accessing data only applies to the data retained solely for compliance with data retention regime. As such, this prohibition does not apply to phone and other data already retained for billing purposes. This data was and will continue to be available for parties in civil litigation to include in applications for discovery.

As noted in the consultation paper, the basic test for determining whether a document (in this case, data) is discoverable, is relevance. In the present context, applications from civil litigants are likely to be third party applications to telecommunications service providers (a non-party to the litigation) for discoverable documents. It is unlikely to be clear prior to such applications whether the documents that are in the possession, power or control of the non-party are relevant. As such, it is easy to see how such applications may quite quickly

[4] Heidi Pett, 'RSPCA and Bankstown council among 61 agencies seeking access to metadata,' ABC News, http://www.abc.net.au/news/2016-01-21/rspca-and-bankstown-council-among-61-agencies/7105940

become routine in a range of legal disputes. This could include family law matters, personal property disputes and applications such as intervention orders.

Compliance with such orders is likely to be costly to telecommunication service providers. The government should consider imposing costs on such applications to act as a deterrent for parties in civil litigation who might otherwise treat such efforts as something similar to a fishing expedition.

Much more importantly, however, is the powerful impact such applications will have on personal privacy. Data retained under the regime provides a surprisingly accurate picture of citizen's personal lives, and unfettered access to such data is highly invasive of Australians' privacy. This should only be reserved for parties dealing with serious crimes, as the prohibition currently facilitates. The impact of a prohibition on access on the civil justice system will always be difficult to predict, but the impact on privacy is clear.

In relation to question two set out in the consultation paper, there are some specific projections that can be made with some confidence. It is Digital Rights Watch's submission that it is highly unlikely that the prohibition (or absence of exemptions) would have a significant impact on copyright infringement litigation. Given the result in the matter of the film 'Dallas Buyers Club', it seems clear that rights holders are unenthusiastic about pursuing infringement cases where there are significant administrative costs associated with doing so. In practice, rights holders have not pursued regimes to protect their rights where it is time consuming and costly, and attempting to access data retained under the regime would likely fall into this category. As such, and in the absences of more fulsome information, we submit that the prohibition under section 187AA would not adversely impact the effective operation of the civil justice system and would have little impact on the material interests of rights-holders in these contexts. Certainly, there is not a clear case that the impact is so significant as to justify the serious invasion of privacy that exceptions to the prohibition are likely to represent.

The appropriate method for determining the prohibition and exceptions under 187AA

Digital Rights Watch submits that any method for determining the extent of the prohibition and any exemptions in relation to accessing data retained for the purpose of this regime should, first and foremost, use a human rights lens.

Australia's human rights obligations provide a relevant set of instruments for analysing the appropriate responsibilities of the government in this situation. The data retention scheme imposes an obligation on telecommunications providers to store information about their users' communications that is either in itself personal data, or that can reveal personal information. The introduction of the scheme is therefore an imposition on the human right to

privacy, generally represented in international documents as the right not to be subjected to arbitrary interference with privacy, family life, home and correspondence.[5]

According to international human rights law, in order for a data retention regime to be legitimate, it must be both necessary to address a legitimate goal and be a proportionate means to achieving that goal.

There are grave doubts about whether and how the very existence of a data retention scheme can be compatible with freedom of expression and privacy rights. The strongest statements, like the 'necessary and proportionate' principles,[6] would prohibit completely the indiscriminate collection of metadata. The European Court of Justice (ECJ) has held that an indiscriminate data retention obligation went beyond what was necessary and proportionate to achieve its objectives to fight 'serious crimes' and was therefore incompatible with the fundamental right to privacy and to data protection.[7] In its most recent decision, the ECJ has reaffirmed this position, explaining that storing such data, which includes text message senders and recipients and call histories, allows for "very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained.'[8]

Even where retention is justified, the UN and Inter-American Special Rapporteurs on Freedom of Expression[9] have warned that access to telecommunications data should only be authorised under the 'most exceptional circumstances'. In the United States, a presidential review of surveillance has recommended that access to data must be strictly limited to national security interests and permitted only with a court order.[10] In a country where warrantless access to metadata about citizens' behaviour raises serious legal and constitutional concerns,[11] a new Presidential Policy Directive requires even surveillance targeted at non-US persons to be used only in relation to national security, cybersecurity, and transnational crime.[12]

---

[5] United Nations. (1948) Universal Declaration of Human Rights, Art 12; United Nations. (1966). International Covenant on Civil and Political Rights, Art 17.

[6] Necessary and Proportionate: International Principles on the Application of Human Rights to Communications Surveillance. (2014, May). Retrieved June 18, 2016, from https://necessaryandproportionate.org/principles

[7] Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, No. C-293/12 and C-594/12 (Grand Chamber, European Court of Justice April 8, 2014). Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0293&rid=1

[8] http://www.dw.com/en/european-court-of-justice-rules-against-mass-data-retention-in-eu/a-36859714

[9] United Nations Special Rapporteur on the Protection and Promotion of the Right to Freedom of Opinion and Expression, & Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights. (2013, June 21). Joint Declaration on surveillance programs and their impact on freedom of expression. Retrieved June 18, 2016, from http://www.oas.org/en/iachr/expression/showarticle.asp?artID=926&lID=1

[10] Review Group on Intelligence and Communications Technologies. (2013). *Liberty and Security in a Changing World*. Retrieved from https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

[11] Donohue, L. K. (2014). Bulk Metadata Collection: Statutory and Constitutional Considerations. *Harvard Journal of Law & Public Policy*, *37*(3), 757.

[12] Obama, B. (2014, January 17). Presidential Policy Directive 28. Retrieved June 18, 2016, from https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities

While it is hard to articulate a definitive standard as to when data retention regimes will be proportionate,[13] a minimal baseline seems relatively clear: measures that are justifiable on national security grounds may not be justifiable for ordinary law enforcement purposes, and access to metadata must be constrained by legitimate judicial authority.

Amendments to current scheme under basis of current justification

Digital Rights Watch believes that the existing legislative scheme is incompatible with the human right to privacy. However, for the purposes of this submission, taking the government's view that the scheme is justifiable on national security grounds, Digital Rights Watch proposes a number of changes to the use and access of retained data for other purposes.

Disclosure of the data retained by the scheme should be permissible only on national security grounds, without exceptions. However, if our submission is not accepted and the Government continues to take the view that there are some civil matters which are sufficiently serious to allow courts hearing those matters to compel disclosure of retained data, those matters must be clearly specified in draft legislation which is then subject to public debate and scrutiny. Delegating decision-making to a Minister is an inappropriate removal of parliamentary and democratic oversight.

The Committee referred to family law proceedings involving violence or international child abduction cases as the kinds of civil proceedings which would warrant disclosure of retained data. First, it should be noted that such matters are already able to be investigated and litigated in a fair manner without access to data retained for the purposes of the regime. Second, if it is the Government's intention that the exceptions be limited to situations such as these, then the legislation should at the very least reflect this intention to limit the possibility of misuse or "scope creep". Given the significant incursion into human rights the regime already represents, a broad discretionary power to prescribe exceptions to non-disclosure is plainly unacceptable. This could take the form of a further procedural step in such applications for this data that balances the seriousness of the civil proceedings and the invasive nature of the data that is the subject of the application.

We submit that section 280(IC)(a) goes far beyond what is necessary and proportionate to achieve national security objectives and that the Government should take the opportunity of this review to remove it from the legislation before the subsection commences.

Digital Rights Watch believes that the data retention regime becomes clearly and unambiguously inconsistent with the human right to privacy at the moment that it requires indiscriminate collection of metadata for anything other than critical national security

[13] Brown, I., Halperin, M. H., Hayes, B., Scott, B., & Vermeulen, M. (2015). Towards Multilateral Standards for Surveillance Reform. *Oxford Internet Institute Discussion Paper*. Retrieved from http://papers.ssrn.com/abstract=2551164

reasons. We urge the Government to ensure that any retained data is not accessible for other purposes.

Digital Rights Watch recommends that the government not issue any exceptions to the prohibition in section 280(1B) of the Telecommunications Act 1997 for any civil proceedings or circumstances.