



**Australian Government**

**Review of whether there should be exceptions to the  
prohibition on civil litigant access to retained  
telecommunications data**

April 2017

## Purpose of the review

This review assesses whether regulations should be made to create exceptions to the prohibition on civil litigants accessing telecommunications data retained solely for the purpose of the mandatory data retention scheme.<sup>1</sup>

The review has been conducted in accordance with Recommendation 23 of the Parliamentary Joint Committee on Intelligence and Security (PJCIS) *Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*,<sup>2</sup> which the Government supported:

*The Committee recommends that the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 be amended to prohibit civil litigants from being able to access telecommunications data that is held by a service provider solely for the purpose of complying with the mandatory data retention regime.*

*To enable appropriate exceptions to this prohibition the Committee recommends that a regulation making power be included.*

*Further, the Committee recommends that the Minister for Communications and the Attorney-General review this measure and report to the Parliament on the findings of that review by the end of the implementation phase of the Bill.*<sup>3</sup>

In its report, the PJCIS indicated that the data retention scheme was established specifically for law enforcement and national security purposes and that as a general principle it would be inappropriate for the data retained under that scheme to be drawn upon as a new source of evidence in civil disputes. However, the PJCIS also indicated that it was aware of the potential for unintended consequences resulting from a prohibition on courts authorising access to data retained under the scheme. The PJCIS indicated that ‘family law proceedings relating to violence or international child abduction cases’ were examples of exceptions that could be considered.<sup>4</sup>

In accordance with the recommendation, the Government inserted section 280(1B) into the *Telecommunications Act 1997* to prohibit telecommunications providers from disclosing data retained solely for the purpose of complying with their data retention obligations in response to subpoenas, notices of disclosure and court orders in connection with civil proceedings. The Government also inserted the recommended regulation making power into the Act that could be used to create exceptions to the prohibition.

---

<sup>1</sup> The mandatory data retention scheme is set out in the *Telecommunications (Interception and Access) Act 1979*.

<sup>2</sup> The full PJCIS Advisory Report is available from [www.aph.gov.au/Parliamentary\\_Business/Committees/Joint/Intelligence\\_and\\_Security/Data\\_Retention/Report](http://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/Data_Retention/Report).

<sup>3</sup> Page 224 of the [PJCIS Advisory Report](#).

<sup>4</sup> Page 223 of the [PJCIS Advisory Report](#).

## Consultation

The Department of Communications and the Arts and the Attorney-General's Department prepared a consultation paper and sought stakeholder views on whether there is a case for regulations to be made, receiving 262 submissions. Public submissions and the consultation paper are available on each Department's website.<sup>5</sup> The Departments also held discussions with major telecommunications providers.

### Summary of submissions

In general, most groups and individuals that made submissions argued that civil litigants should not be permitted to access data retained solely for the purpose of complying with the data retention scheme. Many cited privacy concerns and indicated that making regulations would be inconsistent with the scheme's national security and law enforcement purposes. A small number argued that civil litigants should be able to access the data, or particular types of data, in some circumstances.

**Legal sector:** Members of the legal sector were generally concerned that making exceptions to the prohibition would adversely affect the operations of the courts. There were concerns that exceptions would increase the cost and duration of civil disputes, enabling litigants to waste court resources by seeking large volumes of potentially irrelevant data. It was suggested that the proliferation of documents, particularly electronic documents, is a feature of modern civil litigation, and that this can overwhelm both parties and the courts.<sup>6</sup> The Australian Lawyers Alliance, for example, argued that exceptions 'could add significant time to the preparation of cases, as the data available would be voluminous' and interpreting it during the search for evidence would require additional details like the relevant phone number and locations. It argued that costs could 'escalate dramatically'.<sup>7</sup> Further, many members of the legal sector also raised privacy concerns similar to those expressed by privacy and human rights organisations. The three courts that made submissions noted that retained data could provide useful evidence in certain circumstances.<sup>8</sup>

**Privacy and human rights organisations:** A large number of privacy and human rights stakeholders raised privacy concerns in their submissions. The Australian Privacy Commissioner indicated that if it was considered necessary to create an exception then the scope of such a regulation 'should be drafted as narrowly as possible to achieve the desired policy objective and employ appropriate privacy safeguards'.<sup>9</sup> The Commissioner for Privacy and Data Protection (Victoria) noted that 'a broadening of the original intended purpose of the data retention scheme would serve to further undermine the fundamental right to privacy'.<sup>10</sup> Several organisations expressed the view that data collected for the sole purpose of the data retention scheme is 'data to which neither courts nor litigants would ever have had access without the retention regime, so it does not make sense to say that their proceedings or rights may be impaired if they cannot access it'.<sup>11</sup>

**Telecommunications sector:** Telecommunications providers were generally neutral on whether, as a matter of principle, regulations should be made to allow civil litigants to access retained data. Telstra suggested that one option would be to remove the prohibition, leaving it to the courts to assess the

---

<sup>5</sup> [www.ag.gov.au/Consultations/Pages/Access-to-telecommunications-data-in-civil-proceedings.aspx](http://www.ag.gov.au/Consultations/Pages/Access-to-telecommunications-data-in-civil-proceedings.aspx) and [www.communications.gov.au/departmental-news/consultation-access-telecommunications-data](http://www.communications.gov.au/departmental-news/consultation-access-telecommunications-data)

<sup>6</sup> See, for example, the submission by Albert Ounapuu.

<sup>7</sup> Paragraph 17, page 7 of the submission by the Australian Lawyers Alliance.

<sup>8</sup> Submissions by the Federal Court of Australia (pages 2 and 3), Federal Circuit Court of Australia (page 2) and Family Court of Australia (page 2).

<sup>9</sup> Page 2 of the submission by the Australian Privacy Commissioner (Office of the Australian Information Commissioner).

<sup>10</sup> Page 1 of the submission by the Commissioner for Privacy and Data Protection (Victoria).

<sup>11</sup> Page 5 of the submission by Castan Centre for Human Rights Law.

value of telecommunications data in civil cases.<sup>12</sup> However, providers also indicated that it is already difficult to recover the costs of complying with court orders. They argued that allowing civil litigants access to retained data in certain circumstances would lead to further compliance costs and that if such access were to be provided then existing cost recovery arrangements should be improved.<sup>13</sup> The Australian Communications Consumer Action Network (ACCAN) was concerned that if the costs of processing such requests fell to providers then 'there is a possibility that they will flow down to consumers'.<sup>14</sup> ACCAN also raised general privacy concerns similar to those expressed by privacy and human rights organisations.<sup>15</sup>

**Media sector:** In a joint submission, major media groups<sup>16</sup> argued that regulations had the potential to undermine the confidentiality of journalistic sources and freedom of speech. The groups supported a continuation of the prohibition against civil litigants being able to access this type of data without any exceptions for civil cases.

**Political parties and Members of Parliament:** Most of the submissions received from political parties and Members of Parliament recommended against creating exceptions to the prohibition on privacy grounds. Federal Member for Griffith, Terri Butler MP, recommended against exceptions on privacy and civil liberties grounds and to avoid further increasing the costs of discovery in civil proceedings.<sup>17</sup>

**Government entities and representatives:** The Northern Territory Attorney-General and Minister for Justice, Natasha Fyles, indicated that an exception would place the data at much higher risk of loss or misuse, although it may be useful for proceedings with an important public interest purpose such as those related to criminal proceedings or obtaining a protection order.<sup>18</sup> The Australian Federal Police is of the view that access to telecommunications data should be limited to law enforcement and national security purposes and 'should not be extended to allow use in civil proceedings that lack a law enforcement nexus'. The Queensland Crime and Corruption Commission (CCC Qld)<sup>19</sup> and the ACT Justice and Community Safety Directorate (ACT Directorate)<sup>20</sup> identified proceedings such as proceeds of crime, control orders, child protection orders and apprehended violence orders as potentially appropriate exceptions to the prohibition.

**Individuals:** Of the 217 individuals who made submissions, four expressed support for allowing civil litigants access to the data. Almost all other individuals were strongly against making exceptions, largely because of concerns about privacy. A range of submissions expressed concerns that providing access to retained data for civil proceedings would be an expansion upon the stated national security and law enforcement objectives of the data retention scheme, including in relation to cases involving copyright infringement.

---

<sup>12</sup> Page 2 of the submission by Telstra.

<sup>13</sup> See, for example, pages 4 and 5 of the joint submission by Communications Alliance and the Australian Mobile Telecommunications Association.

<sup>14</sup> Page 6 of the submission by ACCAN.

<sup>15</sup> Page 7 of the submission by ACCAN.

<sup>16</sup> Joint submission by AAP, ABC, APN News and Media, Australian Subscription Television and Radio Association, Bauer Media Group, Commercial Radio Australia, Community Broadcasting Association of Australia, Fairfax Media, Free TV, MEAA, News Corp Australia, NewsMediaWorks, SBS and The West Australian.

<sup>17</sup> Page 1 of the submission by Terri Butler MP.

<sup>18</sup> Pages 1 and 2 of the submission by the Northern Territory Attorney-General and Minister for Justice, Natasha Fyles.

<sup>19</sup> Page 6 of the submission by the Queensland Crime and Corruption Commission.

<sup>20</sup> Page 2 of Attachment A to the submission by the ACT Justice and Community Safety Directorate.

## Findings

### Data accessible to civil litigants

The prohibition preserves civil litigants' access to data that is not retained solely for the purpose of the data retention scheme.<sup>21</sup> Prior to the introduction of the scheme, telecommunications providers were already retaining some of the data that they are required to retain under the scheme, particularly subscriber information and data relating to fixed voice services.<sup>22</sup> The types of data individual providers will be able to disclose to civil litigants will vary depending on providers' past retention practices and the degree to which their operational data is also used to comply with the data retention scheme. The data that can be disclosed will also depend on the degree to which providers use newly retained data for other purposes, although submissions from providers gave no indication of the degree to which they intend to use such data for other purposes.

The courts' powers to order access to relevant telecommunications data in civil proceedings, via subpoenas, notices of disclosure or court orders, are long-standing. The submission from the Family Court of Australia noted that it already deals with information that is highly confidential or commercially sensitive and that a number of safeguards already exist in the subpoena process. These safeguards include that, with some exceptions for interim, ancillary, procedural or other administrative matters, issuing a subpoena requires the permission of the court, and the court will only grant permission where there is a legitimate forensic interest. Even when a subpoena has been issued, a party may object to the subpoena, or to the inspection of a specific document requested in the subpoena. The Family Court of Australia noted that 'where the Court issues a subpoena for production of documents, an application may be made to set aside the subpoena, if, for example, it is oppressive, too wide, ambiguous, "fishing", or conflicts with privilege'.<sup>23</sup> Further, there are restrictions on the use of information obtained via subpoena, and where appropriate the court can apply further conditions or restrictions.

Several submissions expressed concern that it will be left to providers to ascertain whether the data is retained solely for the purpose of complying with the data retention scheme, and that consequently the law may be applied inconsistently or arbitrarily.<sup>24</sup> As indicated above, civil litigants will be able to access different data from different providers depending on the interaction between their business models and information keeping practices. If a provider does not comply with a subpoena to produce information or documents then a court will follow its standard procedures for enforcing compliance. Similarly, if a provider discloses information that is retained solely for the purpose of the data retention scheme then it could be in breach of the *Telecommunications Act 1997*.

### Civil litigants' use of data prior to the prohibition

Submissions revealed limited information about the circumstances in which civil litigants currently seek access to telecommunications data or the circumstances in which they have done so in the past. Under existing arrangements, access can be sought in any number of circumstances provided relevant legal requirements, such as court rules, are met. Similarly, any type of available data could

---

<sup>21</sup> As noted in paragraph 33, page 11 of the Bill's [Supplementary Explanatory Memorandum](#), 'The amendments seek to ensure that access to data that is currently available to claimants and respondents is not reduced or limited, as the prohibition is limited to data held solely for the purposes of compliance with the new data retention obligation and related purposes'.

<sup>22</sup> This finding is supported through consultation with telecommunications providers and also in submissions to the PJCS Inquiry – see, for example, page 1 of the Telstra submission to the PJCS Inquiry, page 10 of the Optus submission to the PJCS Inquiry and pages 120-121 of the [PJCS Advisory Report](#).

<sup>23</sup> Page 3 of submission by the Family Court of Australia.

<sup>24</sup> See, for example, paragraph 12, page 6 of the submission by the Australian Lawyers Alliance.

potentially be accessed, although it appears that requests commonly relate to billing and subscriber records.<sup>25</sup>

Information was sought from telecommunications providers and legal sector stakeholders about the types of civil matters for which telecommunications data had been obtained in the past. No submissions received shed light on that question. Telecommunications providers advised that court documents generally only list the names of the parties, the court and the data requested – they do not identify the type of matter to which they relate. However, it appears that, in relative terms, a modest number of requests for data have been made in civil proceedings in the past when compared with the number of data authorisations made by law enforcement agencies.<sup>26</sup> Figures published by Telstra indicate that in the 2015-16 financial year it responded to 518 court orders which ‘typically... involve a civil dispute that involves individuals or organisations’.<sup>27</sup> This represents less than one per cent of Telstra’s total ‘law enforcement requests’, excluding those from national security agencies.

It is difficult to predict whether requests from civil litigants (volume, type of data requested and the purposes for which requests are made) will change after the prohibition commences.

## Evidence for exceptions

The review received little compelling evidence justifying exceptions to the prohibition in relation to particular types of civil matters. However, contributions from the Australian Federal Police (AFP), the Queensland College of Teachers (QCT), the Queensland Crime and Corruption Commission (CCC Qld), the ACT Justice and Community Safety Directorate (ACT Directorate) and the Law Council of Australia did raise issues for further consideration.

Both the AFP and the CCC Qld indicated that it would be useful for law enforcement-related civil proceedings to be excluded from the prohibition. The AFP gave examples of proceeds of crime proceedings, child protection orders and apprehended violence orders, and the CCC Qld agreed that retained data is of ‘particular importance where civil proceedings are closely linked to a criminal matter’. The AFP and CCC Qld are criminal enforcement agencies under the *Telecommunications (Interception and Access) Act 1979* (TIA Act). Access and use of telecommunications data by enforcement agencies such as the AFP and the CCC Qld is regulated by the TIA Act and separate to the current review.

The QCT indicated in its submission that telecommunications data has been useful to establish facts in disciplinary actions before the Queensland Civil and Administrative Tribunal (such as cases involving a breach of the professional boundary between teacher and student). Because the QCT has an important role in the protection of children by regulating teachers’ conduct, it argued that the disciplinary referrals it makes to the tribunal should be an exception to the prohibition. However, the QCT did not provide details about how telecommunications data has been used in such cases and the role it has played. In addition, it would be open for a police force to access telecommunications data for the purpose of bringing a criminal charge in relation to such conduct if it involved a breach of a criminal law.

The ACT Directorate considered that there may be significant benefit in exceptions for domestic and family violence orders, protection orders and other serious civil proceedings (such as workers compensation, civil penalty and proceeds of crime proceedings, and coronial inquests). The ACT Directorate indicated in its submission that telecommunications data has been sought in these types of cases previously, because these types of proceedings can ‘lead to criminal sanctions, and the

---

<sup>25</sup> See, for example, page 1 of the joint submission by Communications Alliance and the Australian Mobile Telecommunications Association, and page 4 of the submission by the CCC Qld.

<sup>26</sup> See, for example, the submissions by the Federal Court of Australia and the Family Court of Australia.

<sup>27</sup> See [www.telstra.com.au/privacy/transparency](http://www.telstra.com.au/privacy/transparency).

behaviour of concern is often akin to, or overlaps with, criminal conduct'.<sup>28</sup> The ACT Directorate submitted that prohibiting access to telecommunications data in these types of proceedings could potentially be catastrophic, as it could affect family and children's safety. However, like the CCC Qld and the QCT, the ACT Directorate did not provide details on how telecommunications data has been used in these proceedings in the past.

The Law Council of Australia considered the use of telecommunications data in civil cases involving family violence. It indicated that there are difficulties in allowing access in these cases as subpoenas can be issued by administrative staff without judicial consideration, and can involve competing priorities of protecting a victim of family violence and full and frank disclosure between litigants when determining who should be able to access the data. Its preliminary view was that to justify access to retained telecommunications data in situations involving apprehended violence orders, the court must have the ability to assess the merits of granting a court order taking into account the potential danger to the victim in granting access, the privacy of the parties and the seriousness of the alleged behaviour.

The Law Council of Australia also considered access to data in civil child protection proceedings, and for related child location orders made under section 67J of the *Family Law Act 1975*. A location order is an order that requires a person to provide to the court any information they have about the location of a child. Such orders are used to locate and recover children in cases including domestic and international child abduction and are expressed to require compliance 'in spite of anything in any other law'. The Law Council's position was that further evidence would be required to demonstrate the kinds of circumstances where exceptions would be necessary and proportionate in these cases.

Given the limited practical evidence about the degree to which telecommunications data has been useful in these types of matters, it is difficult to determine the strength of the case for access in these circumstances at this time. Further consultation and evidence would be needed to properly assess the case for exceptions to the prohibition in such circumstances. Exceptions could be considered at a later date, should further evidence of need emerge.

## Regulatory impact on telecommunications providers

Once the prohibition commences, telecommunications providers will face an additional administrative cost associated with determining whether the data requested is being retained solely for the purpose of the data retention scheme. Providers advised that in many cases they are currently unable to recover the full cost of considering and responding to court requests. For example, Telstra indicated in its submission that it rarely recovers the cost of producing documents or providing witnesses in response to subpoenas.<sup>29</sup> In addition, providers were concerned that the liability protections they receive for disclosing data to law enforcement agencies do not extend to the disclosure of data to civil litigants.<sup>30</sup>

The introduction of any exceptions to the prohibition could complicate the assessments made by providers when determining whether they can disclose data to civil litigants, and therefore increase costs and legal risks for providers. This is likely to be exacerbated if the exceptions are not appropriately defined or require providers to assess additional criteria.

---

<sup>28</sup> See page 2 of submission by the ACT Directorate.

<sup>29</sup> Page 3 of the submission by Telstra.

<sup>30</sup> Page 4 of the joint submission by Communications Alliance and the Australian Mobile Telecommunications Association and page 3 of the submission by Telstra.

## Conclusions

1. Although there is a history of telecommunications data being obtained to support a modest number of civil cases, the review has received insufficient evidence to sustain a recommendation that regulations be made to allow civil litigants to access data retained solely for the purpose of the data retention scheme.
2. The prohibition preserves civil litigants' access to data that is not retained for the purpose of the data retention scheme while restricting access to data accumulated and used solely for the purpose of the scheme.
3. Should evidence reveal a need for exceptions in the future, regulations could be considered at that time. This would be subject to consultation and involve consideration of privacy issues and the impact on telecommunications providers.
4. It would be open to the Parliamentary Joint Committee on Intelligence and Security to examine the prohibition and regulation making power in 2019 when it undertakes its prescribed statutory review of the data retention scheme.