Australian Government
The Treasury

Screen scraping – policy and regulatory implications

Discussion paper

August 2023

treasury.gov.au

Manager
Media and Speeches Unit
The Treasury
Langton Crescent
Parkes ACT 2600
Email: media@treasury.gov.au

Contents

Consultation Process

Request for feedback and comments

This paper seeks information and views to inform policy development on options for regulating screen scraping practices that involve consumers sharing login details with third parties to access their accounts to collect data to support the provision of products and services.

Questions are included throughout the paper to guide comments. Interested parties may wish to provide responses to some or all of the questions, or to comment on issues more broadly.

While submissions may be lodged electronically or by post, electronic lodgement is preferred. For accessibility reasons, please submit responses sent via email in a Word or RTF format. An additional PDF version may also be submitted.

Publication of submissions and confidentiality

All information (including name and address details) contained in formal submissions will be made available to the public on the Australian Treasury website, unless you indicate that you would like all or part of your submission to remain confidential. Automatically generated confidentiality statements in emails do not suffice for this purpose. Respondents who would like part of their submission to remain confidential should provide this information marked as such in a separate attachment.

Legal requirements, such as those imposed by the *Freedom of Information Act 1982*, may affect the confidentiality of your submission.

If you would like to share information and views that may be sensitive, you are welcome to indicate that you would like all or part of your submission to remain confidential. Treasury also welcomes the opportunity to discuss your views in a meeting.

Closing date for submissions: COB Wednesday 25 October 2023

Email	data@treasury.gov.au
Mail	Consumer Data Right Policy and Engagement Branch Market Conduct and Digital Division The Treasury Langton Crescent PARKES ACT 2600
Enquiries	Enquiries can be directed to data@treasury.gov.au Media enquiries can be directed to media@treasury.gov.au

Screen scraping – policy and regulatory implications

Background

Screen scraping, also known as digital data capture, is a technology that collects displayed data to be used for a specific purpose. Screen scraping may be used to support a range of activities, such as the collection of data from public-facing webpages or internal use within a business to reconcile accounts.

This discussion paper focuses on the form of screen scraping that involves consumers sharing their personal login details with third parties, such as internet banking login details. These third parties collect point-in-time data to provide the consumer with a service. This use of screen scraping is particularly prevalent in financial services and may be used by some banks, lenders, mortgage brokers, financial advisers, accounting services and more, but is inconsistent with best practice cyber security advice and may pose risks to consumers due to how the data is collected and handled.

Cyber security and consumer protection risks of screen scraping practices have been raised in various reviews and inquiries, which include the:

- 2017 Review into Open Banking in Australia and the 2020 Inquiry into Future Directions for the Consumer Data Right (in the context of payment initiation), both by independent reviewer Scott Farrell.
- 2019-2021 inquiry by the Senate Select Committee on Financial Technology and Regulatory Technology (referred to as the Senate Select Committee Inquiry on Fintech and Regtech).[1]
- 2022 Statutory Review of the CDR (the Statutory Review) by independent reviewer Elizabeth Kelly PSM.[2]
- submissions to the Review of the *Privacy Act 1988* (Privacy Act Review). The Privacy Act Review report was released in February 2023.

In this context, the Consumer Data Right (CDR) has been discussed as a safer way for consumers to digitally share their data to receive a service compared to screen scraping, as it does not require consumers to share their login details and can offer protections around what data is collected and how this data can be used and disclosed. Of note, recommendation 2.1 of the Statutory Review stated that:

> *'screen scraping should be banned in the near future in sectors where the CDR is a viable alternative. Importantly, the Government should clearly signal when and how the implementation of the ban would take effect. This would provide certainty and adequate time for businesses to transition, along with stronger incentives to invest in moving to the CDR.'*

On 7 June 2023, the Government released its statement in response to the Statutory Review,[3] which stated that:

> *'the Government will consult on policy options to regulate screen scraping commencing in the banking sector, starting with the release of a discussion paper in the second half of 2023.'*

[1] Screen scraping was considered in detail in the Committee's interim report from September 2020. On 18 March 2021, the Senate Select Committee on Financial Technology and Regulatory Technology was renamed to the Select Committee on Australia as a Technology and Financial Centre.
[2] Elizabeth Kelly, Statutory Review of the CDR, 29 September 2022.
[3] Treasury, Government statement in response to the Statutory Review of the CDR, 7 June 2023.

During consultations to date, some stakeholders have expressed strong support for the continued use of screen scraping practices in parallel with the CDR. Other stakeholders have advocated against the continuing use of screen scraping in the financial services sector due to the risks to consumers, arguing that without having a clear endpoint for screen scraping there is little incentive to adopt the CDR as an alternative.

This discussion paper aims to gather further information and views to inform policy options for regulating screen scraping. The screen scraping market is complex, with different use cases capturing a range of different data. Before the recommendation in the Statutory Review could be implemented, it is important to understand the operation of the screen scraping market in Australia and the likely impact of regulation.

How is screen scraping currently used?

Screen scraping technology can be used for both 'read' and 'write' access. 'Read access' enables the scraper to access the consumer's account to see and collect data, which can be converted or aggregated to generate the required product or service. Under 'write access', after the consumer provides their login details, the scraper can access data from the consumer's account and take actions on the consumer's behalf.

Common use cases for screen scraping include:

- the lending application process, where a consumer shares their banking data with a lender or a mortgage broker to facilitate checks for a lender to meet responsible lending obligations, facilitate a lender's creditworthiness assessment (including informing pricing and risk assessment models), and to pre-fill loan applications. Data can be shared for different types of lending, from larger loans (such as mortgages and business loans) to small amount credit contracts (including payday loans) and consumer leases.[4]
- financial management applications that use screen scraping technology to read consumer data across several banking platforms to create an aggregate financial dashboard for the consumer.
- accounting software services that use screen scraping technology to automatically reconcile a business' financial accounts and streamline bookkeeping processes.
- financial technology (FinTech) services. One example is an investment platform providing a round-up service that links to a customer's bank account and automatically invests the spare change from a transaction for the consumer.

Screen scraping may also be used to support identity verification of consumers, for example, by sharing login details for a bank account that a bank has already conducted identity verification upon.

Consistent with the use cases outlined above, stakeholders have noted that screen scraping is most commonly used to obtain banking data. Beyond banking, the practice may also be used to share data from other accounts, such as superannuation and non-bank lending data, or the sharing of MyGov details to provide information about Centrepay deductions, which are regular deductions from Centrelink payments.[5]

[4] The *National Consumer Credit Protection Act 2009* requires payday lenders and consumer lessors to obtain 90 days of banking transaction data when assessing a loan application. Other credit providers often also choose or are required to get banking transaction data to gather and verify financial information pursuant to responsible lending obligations.
[5] While we note this activity can occur in the market, sharing MyGov details (which would include undertaking two-factor authentication) violates MyGov's Terms of Use – refer to 'Keep your MyGov account safe.'

It is common for many businesses, including mortgage brokers, to use third party data services to perform the screen scraping activity for them. Some companies use screen scraping for one-off access to customer information to create a point-in-time result. For example, when screen scraping is used in the lending sector the data is often accessed as a one-off to aggregate point-in-time transaction data. Other companies may use screen scraping to access customers' accounts on an ongoing basis. For example, offering personalised financial management or investment applications requires accurate and updated transaction data to ensure a holistic view of the consumer's finances; and to conduct subsequent responsible lending assessments when credit limit increases are sought.

1. What screen scraping practices are you aware of or involved in?
    a) What is the scope and purpose of the data that is captured? Is the data that is captured only banking data, or does it include data from other sectors?
    b) What steps do consumers, screen scraping service providers and businesses using screen scraping take in the screen scraping process? What information is provided to consumers through the process?
    c) When is the consumer's data accessed as a one-off, and when is longer-term or ongoing access obtained? Where ongoing access is in place, how are consumers made aware of this and can they cancel access at a later point?
    d) Do you use screen scraping for purposes other than data collection (for example to undertake actions on behalf of a customer)?

What are the risks of screen scraping?

When consumers disclose their login details with a third party, there are associated risks to the consumer – for example, the third party has a consumer's login details, can have access to a broad range of a consumer's data, and can potentially have ongoing access to the consumer's accounts in the future. This section explores some of the key risks to consumers of sharing their login details through screen scraping. These risks reflect concerns that have been raised in previous consultation processes, including the Statutory Review and the Inquiry on Fintech and Regtech.

Counters good online security practices

Fighting scams and fraud is one of the Government's priorities.[6] Consumer awareness of online scams and fraud has increased, and many consumers are wary of handing over their passwords and login details.

Asking consumers to engage in any practice in which they disclose login and password information to third parties runs counter to IT security practices, advice provided by the Australian Government (for example, advice on the ACCC's Scamwatch website to not share login details), banks' terms and conditions, and MyGov's Terms of Use. Against a backdrop of heightened security awareness, it may be difficult for some consumers to navigate what actions are right for them if they are given mixed messages about the risks associated with sharing their login details.

[6] Assistant Treasurer, Fighting back against scammer scourge - Government announces new anti-scams centre media release, 15 May 2023. The Government's work on scams and cyber security is also summarised in the Strategic Plan for Australia's Payments System.

Moreover, this use of screen scraping expands the number of parties who hold consumer login details, potentially increasing opportunities for other malicious activity, such as phishing attacks, and increasing consumers' vulnerability to scams.

Activities by banks

Stakeholders have noted that the use of screen scraping counters the security protocols of many Australian banks, which generally stipulate in their terms and conditions that customers must not share their login details. Banks perform due diligence activities to verify customer identification to protect consumers and organisations against fraudulent activity. During the Inquiry into Fintech and Regtech, the Commonwealth Bank stated that where the bank identifies that a third party is accessing a customer's account, as is done through screen scraping, it takes steps to warn the customer of the potential risk they are taking.[7] Banks have also heightened their security through multifactor authentication;[8] this additional protection barrier can interrupt screen scraping processes and inhibit the technology from accessing that site.

Limited regulation and effect on vulnerable consumers

Screen scraping is not explicitly regulated. Companies may have broader obligations under frameworks like the *Privacy Act 1988* (Privacy Act) related to the collection and handling of personal information and the handling of collected data,[9] and their behaviour may also be bound by various misleading and deceptive conduct provisions.[10] The *National Consumer Credit Protection Act 2009* includes some information protections, but these only apply to small amount credit contracts and consumer leases and do not apply to other forms of consumer credit.

Consumers may not always understand when they are using services that rely on screen scraping, nor the consequences of doing so and any associated risks. For example, it may be unclear to consumers whether data collected will be disclosed to other parties or if service providers may have ongoing access to their account. Because screen scraping involves consumers providing account login details, they may also have little control over what specific data and access the third party may have and how the consumer can end the arrangement.

Banking password disclosure risks in the event of a data breach

In the Senate Select Committee Inquiry into Fintech and Regtech, some stakeholders argued that if any screen scraping providers experience data breaches in the future, large volumes of banking login details or passwords could be exposed. Some providers of screen scraping services noted that they take data security extremely seriously and have banking-level information security measures given their business model and role in the market. While Treasury understands that there have been no reported large-scale cyber security breaches of screen scraping providers to date, it is expected that there would be significant negative consequences for consumers if a data breach involving the loss of consumers' banking login details or passwords were ever to occur.

[7] Commonwealth Bank, as noted in the Select Committee on Financial Technology and Regulatory Technology (aph.gov.au)
[8] For example, Macquarie Bank notes that screen scraping applications will experience issues following the introduction of multi-factor authentication: 'Sharing banking details with third-party applications'.
[9] The Privacy Act currently does not apply to small business operators (entities with an annual turnover of $3m or less), subject to certain exceptions. This was considered in the recent Review of the Privacy Act.
[10] For example, relevant misleading and deceptive conduct provisions to prevent unconscionable conduct in the *Competition and Consumer Act 2010*, *National Consumer Credit Protection Act 2009*, and *Australian Securities and Investments Commission Act 2001*. Commonwealth or state criminal laws may apply if intent of deception or fraud is involved.

Loss of consumer protections under the ePayments code

Consumers who share their login details through screen scraping may lose protections available to them under the ePayments Code to be indemnified for losses caused by unauthorised transactions.[11] The ePayments Code notes that if a consumer discloses a passcode, and the entity subscribing to the Code (e.g. a bank) can prove on the balance of probability that the consumer contributed to a loss by breaching the passcode security requirements, the bank is not required to indemnify the user for that loss.[12] ASIC noted in its latest review of the ePayments Code that consumers use screen scrapers at their own risk, should it amount to 'disclosure' of a passcode.[13]

It should be noted that subscription to the ePayments Code is currently voluntary and the Government intends to consult further to determine how the Code should be updated and brought into regulation.[14]

2. Are there any other risks to consumers from sharing their login details through screen scraping?
3. Do you have any data, case studies, or further information about the risks of consumers sharing their login details through screen scraping?
4. Could you provide any examples of actions your organisation takes to prevent or block screen scraping (if you hold the consumer's data, such as a bank), or when your company's use of screen scraping has been blocked (if you provide screen scraping services or you partner with a screen scraper to provide your services), and why?
5. Could you provide any examples of how your organisation or entities you partner with manage the risks associated with screen scraping?

Reforms and reviews related to the screen scraping market

While there is no specific regulation of screen scraping, numerous legal frameworks and reforms may impact its use. Key Government reforms and reviews related to screen scraping practices are outlined below. Treasury welcomes information on other key frameworks, reviews or reforms closely related to screen scraping that should be considered in policy development.

Reforms to responsible lending obligations

Screen scraping is currently widely used in the lending sector to assess a consumer's financial position, including in for payday lending.

[11] The ePayments Code is a voluntary code that applies to electronic payments including ATM, EFTPOS, credit card, online payments, internet and mobile banking. The code is administered by ASIC. Amongst other protections, the code establishes processes for unauthorised transactions and mistaken payments. Most banks, credit unions and building societies currently subscribe to the ePayments Code, along with a small number of non-banking businesses. The Government plans to consult further to determine how the ePayments Code should be updated and brought into regulation.
[12] Refer to clauses 11 and 12 in particular.
[13] ASIC, Report 718: Response to submissions on CP 341 Review of the ePayments Code: Further Consultation, 7 March 2022. Note that the mere use of a screen scraping and disclosure of one's passcode to the provider does not necessarily lead to liability for an unauthorised transaction – the subscriber (e.g. bank) must prove that the disclosure of the passcode to the screen scraper contributed to the unauthorised transaction.
[14] Treasury, A Strategic Plan for Australia's Payments System, 7 June 2023

In May 2023, the Assistant Treasurer announced reforms to extend responsible lending obligations to Buy Now Pay Later products to better protect consumers using these products. Treasury is working closely with the industry and with consumer groups on the details of the reforms.[15]

Once responsible lending obligations apply to Buy Now Pay Later products, providers may need to collect or verify a consumer's financial circumstances using banking data, similar to existing processes for other regulated credit products. The online nature of most Buy Now Pay Later products will highlight the need for user-friendly, real-time digital access to banking data. Some Buy Now Pay Later providers may seek to use screen scraping or the CDR to meet responsible lending obligations.

Privacy Act Review

The Privacy Act is Australia's primary legislation protecting individuals' personal information. The Privacy Act Review Report, which was released in February 2023, made a range of proposals to strengthen protections and address unsafe uses of personal information. Key proposals that may have implications for the use of screen scraping include the recommended introduction of a new 'fair and reasonable' test for handling personal information and requirements to conduct Privacy Impact Assessments for activities with high privacy risks. The Privacy Act Review Report also proposed removing the small business exemption, meaning that Privacy Act requirements would apply to a much broader range of private sector organisations. The Government is considering its response to the report, following further public consultation that commenced in February 2023.[16]

Other Government measures

Consideration of the use of screen scraping is consistent with the Government's priorities to enhance the security and protection of consumers. The Government is undertaking various measures across the economy, including:

- Combating scams – In the 2023-24 Budget, the Government announced a package to combat scams and online fraud headlined by the establishment of a National Anti-Scam Centre.[17]
- Cyber Security Strategy – The Government is developing the 2023-2030 Australian Cyber Security Strategy to lead a nationally coordinated approach to build cyber security and resilience.[18]
- Digital ID – The Government invested $26.9 million in the 2023-24 Budget to expand Digital ID to increase efficiency and consumer protection, reduce fraud, and make it easier for people to access services online.[19]
- Future consultation on mandating the ePayments Code – As outlined above, one of the risks of consumers using screen scraping is that they may lose protections under the ePayments Code. The ePayments Code is presently a voluntary code of practice, currently subscribed by most banks, credit unions and building societies, along with a small number of non-banking businesses. The Government's Strategic Plan for Australia's Payments System includes consultation in 2025-26 to determine how the ePayments Code should be updated and brought into regulation.

[15] Assistant Treasurer's address to the Responsible Lending and Borrowing Summit, 22 May 2023
[16] Attorney-General's Department, Government response to the Privacy Act Review Report, 16 February 2023
[17] Assistant Treasurer, Fighting back against scammer scourge - Government announces new anti-scams centre media release, 15 May 2023
[18] Minister for Home Affairs, Expert Advisory Board appointed as development of new Cyber Security Strategy begins media release, 8 December 2022
[19] Australian Budget 2023-24, Growing the Economy

International developments in screen scraping

The regulation of screen scraping practices has been considered globally. For example, under the EU's revised Payment Services Directive (known as PSD2) and under the UK's Open Banking framework, screen scraping to digitally capture data is not prohibited, as long as screen scrapers identify themselves to the data holder.[20] Screen scraping that impersonates the customer, such as making payments with no indication that transactions are being initiated by a third party, is prohibited.

6. Are there other proposed reforms or legal frameworks that relate to the use of screen scraping?
7. Are there any other international developments that should be considered?

The Consumer Data Right

The CDR is a data portability scheme that enables consumers to share the data that Australian businesses hold about them for their own benefit. It is a data sharing option that is safer for consumers than screen scraping as it does not require consumers to share their login details and offers protections around what data is collected and how this data can be used and disclosed.

Practically, the CDR uses application programming interfaces (APIs) that facilitate standard communication and data transfers directly between different systems. Consumer data is shared by:

- A consumer providing consent to a data recipient requesting a disclosure of their CDR data,
- The data recipient then requesting access to that consumer's CDR data from the data holder,
- The data holder obtaining the consumer's authorisation to disclose the data, and
- CDR data being automatically shared with the data recipient and used to provide a product or service in accordance with the consumer's consent.

The CDR commenced implementation in the banking sector in July 2020, and data sharing in banking now covers nearly 100 per cent of the sector as measured by the share of household deposits. CDR implementation in the energy sector commenced in November 2022. The Government also committed to expanding the CDR into the non-bank lending sector as part of the 2023-24 Budget. On 25 August 2023, draft amendments to the *Competition and Consumer (Consumer Data Right) Rules 2020* to extend the CDR to the non-bank lending sector were released for consultation.[21]

Unlike screen scraping, consumer protections are a core part of the CDR's legal framework. Key features include:

- Data holders can only share data when consumers have consented to it being shared for a specific purpose, and consumers may withdraw this consent at any time.
- An Accredited Data Recipient (ADR) must comply with a data minimisation principle when collecting or using CDR data.[22]

[20] Regulatory technical standards for strong customer authentication and common and secure open standards of communication, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R0389, Article 30(1)(a).
[21] Consultation on CDR rules – expansion to the non-bank lending sector
[22] The data minimisation principle is outlined in the CDR Rules and requires that accredited persons must not seek to collect data beyond that reasonably required to provide the good or service to which a consumer has consented.

- CDR legislation includes 13 legally binding privacy safeguards that set out privacy obligations for users of the scheme, including covering the collection, use, disclosure, quality and correction of CDR data. Other safeguards restrict the use of CDR data for direct marketing and require accredited data recipients to delete or de-identify data when it is no longer needed.[23]
- There are substantial civil penalties for non-compliance with CDR legislation, enforced by the Australian Competition and Consumer Commission and the Office of the Australian Information Commissioner.

The CDR requires all entities that are designated as data holders to share data with ADRs if the consumer requests it. The CDR also offers consistency and standardisation in access to data sharing across entities. Unlike screen scraping, changes to a data holder's IT platform, such as a modifications to the bank's user interface, do not require participants to re-write scripts to re-establish a connection. Some stakeholders have suggested that these characteristics make the CDR a more stable data-sharing option than screen scraping.

The Statutory Review found that while the CDR provides a safer alternative to screen scraping, submissions noted a number of reasons why some businesses have continued to use screen scraping despite the possibility of receiving data through the CDR. Reasons raised during the Statutory Review included the ease and lower cost of implementation of screen scraping and the quality of CDR data.

The Government's statement in response to the Statutory Review outlined its focus on supporting the maturity of the CDR. Improving CDR system functionality is one of the Government's priorities to open up use cases and drive benefits for consumers. Work to enhance functionality of the CDR includes, but is not limited to:

- Amendments to the CDR Rules to support business consumer participation. The Statutory Review observed that 'many business consumers are unlikely to make the switch from unsafe but more convenient alternatives like screen scraping until the CDR can meet their needs and provide a comparable service'. On 21 July 2023, the Government announced amendments to the CDR Rules to allow businesses to more easily and safely share their CDR data with third parties outside the CDR, such as bookkeepers and accounting software providers.[24] These changes will support business consumers to access better advice more efficiently. As the CDR develops, other opportunities to enhance business consumer use of the CDR will be considered.
- Simplifying the consent process. The Statutory Review found that complex consent processes may limit participation in the CDR (refer to Finding 2.2). On 25 August 2023, Treasury and the Data Standards Body (DSB) released a design paper to consult on proposals aimed at simplifying the CDR consent rules and standards to support a better consumer experience while maintaining key consumer protections.[25]
- Operational enhancements to the CDR Rules. Treasury has been engaging with stakeholders about whether the CDR Rules are fit-for-purpose, including through a formal consultation in late 2022. On 25 August 2023, Treasury released a design paper to consult on proposals aimed at ensuring the CDR Rules are fit-for-purpose and support the effective functioning of the CDR.[26]
- Data quality improvements. The Statutory Review found that improving CDR data quality should be a focus. Following the Statutory Review, the ACCC ran a public consultation process on

[23] The Office of the Australian Information Commissioner has published a brief summary of each privacy safeguard as well as guidelines for each safeguard.
[24] Assistant Treasurer, Small business and customer data to be safer under CDR improvements media release, 21 July 2023 and Competition and Consumer (Consumer Data Right) Amendment Rules (No.1) 2023.
[25] Consultation on CDR rules – Consent Review and operational enhancements design papers
[26] Ibid.

improving data quality, and on 5 April 2023, published its findings and the actions it will take.[27] The Government statement in response to the Statutory Review recognised the importance of ensuring the data shared between data holders and data recipients is accurate and reliable. It stated that the ACCC will continue to engage with industry representatives to improve data quality.

- Authentication Uplift. The CDR authentication uplift work led by the Data Standards Body seeks to improve the consumer experience of authenticating in CDR while maintaining financial grade security.

We are aware that different industry members are at different points in the CDR journey – some are voluntarily using the CDR and have encouraged others to move to the CDR,[28] some may be offering both screen scraping and CDR, others are continuing to use screen scraping for now, and others may not have plans to use the CDR. We are also aware that the use of screen scraping is currently well integrated in some industry sectors. For example, there appears to be low uptake of the CDR in the credit industry for responsible lending obligations. This could be because the CDR is relatively new, has higher costs compared to screen scraping, or due to the CDR's requirements around data handling and consent.

The questions below seek to understand current factors affecting choices on the use of screen scraping or the CDR as an alternative, as well as views on the recommendation in the Statutory Review.

8. What are your views on the comparability of screen scraping and the CDR?
   a) Can you provide examples of data that is being accessed through screen scraping that cannot currently be accessed using the CDR or vice versa?
   b) Are there particular restrictions related to data use and disclosure under the CDR that influence choices to continue using screen scraping, or vice versa?
   c) Are there requirements in other regulatory frameworks that affect the viability of CDR as an alternative to screen scraping?
   d) Can you provide suggestions on how the CDR framework could be adjusted so that it is a more viable alternative to screen scraping?
9. The Statutory Review recommended that screen scraping should be banned in the near future in sectors where the CDR is a viable alternative.
   a) How should the Government determine if the CDR is a viable alternative?
   b) What are your views on a ban on screen scraping where the CDR is a viable alternative?
   c) What timeframe would be required for an industry transition away from screen scraping and why?

[27] ACCC, Data Quality in the CDR – Findings from stakeholder consultation, 5 April 2023
[28] Basiq, The Future is Now. Commit to Open Banking, 8 December 2022