Screen scraping – policy and regulatory implications

ACCC Submission

October 2023

Introduction and Role of the ACCC

1. The Australian Competition and Consumer Commission (ACCC) welcomes the opportunity to comment on Treasury's discussion paper, *Screen scraping – policy and regulatory implications* (August 2023).

2. The ACCC is an independent Commonwealth statutory agency that promotes competition, fair trading and product safety for the benefit of consumers, businesses, and the Australian community. The ACCC's primary responsibilities are to enforce compliance with the competition, consumer protection, fair trading, and product safety provisions of the *Competition and Consumer Act 2010* (Cth) (CCA), regulate national infrastructure and undertake market studies.

3. On 10 February 2020, the Australian Government directed the ACCC to conduct an inquiry into markets for the supply of digital platform services, including the data practices of both digital platform service providers and data brokers. On 10 July 2023, the ACCC released an issues paper seeking views from interested stakeholders on the nature of the data broker industry in Australia and any related competition and consumer issues that may arise.[1] This issues paper will inform the eighth interim report of the Digital Platform Services Inquiry, due to the Treasurer by 31 March 2024. Amongst other things, this report will examine the various methods used by firms to collect consumer data.

4. The ACCC's Consumer Data Right (CDR) roles include accrediting potential data recipients, establishing and maintaining a Register of accredited persons and data holders, assessing applications for exemption from CDR obligations, monitoring compliance and taking enforcement action in collaboration with the Office of the Australian Information Commissioner (OAIC), and providing guidance to stakeholders about their obligations under the CDR. The ACCC also plans, designs, builds, tests, manages and secures enabling technologies for the CDR. As implementer and regulator of the CDR, the ACCC looks forward to working with Treasury, the Data Standards Body and the OAIC to continue to enhance CDR functionality and support CDR as a safe alternative to other data sharing methods.

Executive summary

5. Screen scraping is a data collection technology that extracts displayed data to be used for a specific purpose. The discussion paper, and the ACCC's comments in this submission, focus on the form of screen scraping that involves consumers sharing their personal login details with third parties, so that those third parties can collect data to provide the consumer with a service.

6. The ACCC submits that screen scraping through the sharing of login details puts consumers' data at risk of misuse. The third party conducting the screen scraping gains access to a broad range of consumer data, with consumers having limited control over how the data is collected and handled. Beyond the risk to consumer data, the ACCC is concerned that the act of encouraging consumers to agree to screen scraping in the financial services sector may induce consumers to breach the terms and conditions of their contracts with their banks. It also exposes consumers to the risk of reduced protections under the ePayments Code, in the event they experience a loss associated with an unauthorised transaction. Of significant concern, screen scraping encourages

[1] See ACCC media release on the release of the issues paper on the data broker industry

consumers to normalise the behaviour of sharing login details with third parties, leaving them vulnerable to scams.

7. Noting these risks, the ACCC supports in principle a ban on screen scraping in sectors where CDR is a viable alternative. We encourage the Government to implement a ban promptly. This will encourage increased take up of CDR, thereby ensuring consumers have greater control and protections when accessing products and services that use their data. The ACCC's submission reflects on the concept of CDR as a viable alternative to screen scraping and submits that CDR should be considered a viable alternative by default, in sectors where it has been rolled out.

8. CDR offers a safer way for consumers to digitally share their data when compared to screen scraping, as it does not require consumers to share their login details with third parties. The CDR consent process aims to ensure that consumers are aware of what they are consenting to when they agree to share their data with a third party. CDR also offers explicit protections in relation to the use and collection of data. The third parties accessing data through the CDR must be accredited and there are rules governing how these third parties can use data to provide a product or service to a consumer (which include privacy and security protections).

9. Enhancing CDR functionality without compromising consumer protections, supporting its maturity and broadening its coverage into new sectors will assist to promote CDR as the preferred data sharing option as a ban on screen scraping is implemented. It is important that the CDR program be positioned as such an alternative, offering consumers comparable scope and functionality to screen scraping, while providing them with greater consumer protections and control.

Support for a move away from screen scraping

10. The ACCC supports recommendation 2.1 of the Statutory Review into the CDR that screen scraping be banned in the near future in sectors where the CDR is a viable alternative, and that the Government clearly signal when and how a ban would take effect.[2] The ACCC encourages the prompt implementation of a ban.

11. The ACCC agrees that screen scraping is inconsistent with best practice cyber security advice and may put consumers and their data at risk. The need for a consumer to share personal login details with a third party means the third party gains access to a broad range of consumer data, and may have this access beyond what is reasonably needed to fulfil the specific purpose. Consumers who don't change their login details after consenting to screen scraping risk relinquishing control over how and when their data is accessed. The limited regulation of how screen-scraped data is collected, handled and used means consumers using screen scraping services have reduced control over what happens to their data once it is collected.

12. The ACCC is concerned that screen scraping encourages consumer behaviour that may result in detrimental outcomes beyond the misuse of their data. For example, the act of encouraging consumers to feel comfortable divulging login details may increase consumers' vulnerability to scams. Consumers who provide their banking login details to third parties for the purposes of screen scraping are also acting contrary to banks'

[2] Elizabeth Kelly, *Statutory Review of the CDR*, 29 September 2022, page 12.

customer terms and conditions.[3] In addition, consumers engaging in screen scraping may not be entitled to recover lost funds as a result of an unauthorised transaction under the ePayments Code, in the event the use of a screen scraping service amounts to a disclosure of a consumer's passcode and it can be proven on the balance of probability that the use of that service contributed to the loss.[4]

13. We note that the Australian Government's Roadmap for Australia's Payments System proposes that consultation on introducing supporting regulations for mandating the ePayments Code be conducted in 2025-26.[5] As part of this consultation we encourage consideration of whether the potential for reduced protections in the ePayments Code where screen scraping is used is an appropriate outcome for consumers. This is particularly the case in circumstances where providers in the industry to be covered by the Code (i.e., financial services providers) may encourage the use of screen scraping as a legitimate way to access consumer data.

14. The CDR is a safer way for consumers to digitally share their data as it does not require the sharing of login details with third parties. Rather, CDR offers explicit protections in relation to how consumer data is collected, used and disclosed by requiring third parties to be accredited in order to securely access a consumer's data with the consumer's express consent.[6]

15. Central to this is the CDR consent process, which is designed to ensure that third party requests for data are transparent and that consumers understand what they are consenting to when they agree to share their data. Accredited data recipients (ADRs) must collect and use only the data required to provide the consumer with the service requested and there are rules governing the handling of the consumer's data when the provision of the service ends.

Use of screen scraping in sectors where CDR is available

16. We acknowledge that, to progress to a transition away from screen scraping, further analysis is required to understand the extent to which screen scraping services are being used – including frequency of use; the circumstances of use; and the number of consumers in Australia who share their data using screen scraping. While the ACCC supports a transition away from screen scraping, we note that some consumers may be familiar with and/or reliant on this method of data sharing, given its use in the financial sector to obtain banking and other data.

17. We encourage Treasury to give further consideration to why and to what extent screen scraping is being used in sectors where CDR is available, and whether changes or enhancements to CDR – beyond those already being considered – could promote a transition from screen scraping to CDR.

18. For example, we are aware of services that currently use a consumer's banking, superannuation and shares portfolio data to create a complete picture of a consumer's financial situation. In such situations, a combination of CDR and screen scraping may be

---

3 The Senate, *Select Committee on Financial Technology and Regulatory Technology*, Interim report, September 2020, pp. 143-144.

4 See ASIC, *Review of the ePayments Code: Further consultation*, May 2021, pp. 35-36.

5 See Roadmap for Australia's Payments System.

6 While third parties must be accredited to access a consumer's data, the CDR provides options for data to be on-disclosed to unaccredited parties. For example, the CDR representative model allows an unaccredited person to enter into a 'CDR representative arrangement' with an unrestricted accredited person to access the CDR and use consumer data without being accredited.

needed to access data, as the scope of the data required for the service is greater than what the CDR can currently provide.

19. To offer the enhanced protections of CDR, participants are required to build systems that comply with detailed privacy and information security requirements. This affords significant benefits – ADRs and other parties using CDR data can be confident that when complying with CDR requirements they are providing safe and secure services to consumers, and consumers can be assured that their data is safe and secure when they engage with CDR participants.
20. However, the ACCC notes that because of the enhanced protections afforded by CDR and the system build this requires, it is unlikely to be able to compete with screen scraping on a cost basis alone. Without a clear endpoint for screen scraping there may remain a commercial disincentive for businesses to adopt CDR as an alternative, despite its benefits.

Use of screen scraping alongside CDR

21. The ACCC is aware of anecdotal reports that some ADRs in the banking sector are offering services that use screen scraping alongside CDR. While this practice is not prohibited, we note that it may be confusing for consumers to use a service utilising two data sharing mechanisms. This confusion may arise because the protections offered by CDR necessitate a more detailed consent process for consumers, compared to obtaining data using screen scraping, a process with limited regulation. Some consumers have expressed confusion in circumstances where an ADR is providing services using the CDR logo, and appears to be applying CDR consent processes, but is also asking for the consumer's login details (potentially to obtain data not available via CDR).
22. Where screen scraping sits alongside CDR as a data sharing mechanism, it is important that ADRs do not mislead consumers as to the consents they are entering into and their rights under the CDR framework.[7] To this end, the ACCC supports Treasury's Consent Review and, in particular, consideration of the need for further guidance on how CDR consents may be requested where non-CDR permissions, consents, or agreements are requested for the same service. The ACCC's submission to the Consent Review provides detailed comments on this issue.

CDR as a viable alternative

23. The ACCC submits that where CDR is available, it should be considered the preferred data sharing mechanism over alternatives such as screen scraping. That is, once CDR has been rolled out in a sector, it should be considered a viable alternative to screen scraping, and screen scraping should be banned in that sector. This should be the default position, with further consideration given to the need for appropriate exceptions[8] or sector-specific divergences as a ban is implemented. This will drive CDR uptake and improve protections for consumers sharing their data.
24. While our position is that CDR should by default be considered a viable alternative to screen scraping once it has been rolled out in a sector, the ACCC acknowledges that Treasury may wish to determine an appropriate benchmark for CDR to be considered a 'viable alternative'. Treasury could consider whether it is appropriate to use quantitative metrics on CDR performance, such as data holder platform availability or the number of

---

7 See ACCC Guidance on screen scraping.

8 For example, there may be non-commercial applications, such as academic research, where screen scraping is a useful tool. The ACCC welcomes Treasury's consultation on these issues.

data holder brands providing data to set a benchmark for sectoral coverage.[9] Qualitative measurements such as consumer sentiment on ease of CDR data sharing could supplement the case for CDR as a viable alternative in a sector. It may also be possible to conduct trials or sampling to compare the results of using CDR to provide a service compared to using screen scraping – i.e., to establish that similar services could be provided using CDR.

25. While the ACCC supports in principle a ban on screen scraping where CDR is a viable alternative, we recognise it is likely that screen scraping will continue to exist in sectors where there is no CDR coverage. In the medium to long term, the ACCC notes that enhancing both the CDR's functionality and coverage into new sectors will solidify CDR as a viable alternative to screen scraping. The ACCC acknowledges the significant body of work Treasury is undertaking with this aim in mind.
26. While future developments may increase interest in CDR, the ACCC emphasises the importance of ensuring any changes do not compromise the safety and security of CDR data sharing, or the robust nature of the CDR consent process. It is important that CDR maintain its reputation as a safe and reliable way to share data where the consumer is in control. This will ensure CDR can position itself as not just a viable alternative, but also the preferable alternative to screen scraping.
27. The ACCC notes that as the CDR has grown, strengthening the quality of CDR data has become increasingly important. The ACCC is treating data quality compliance as priority conduct for its CDR compliance and enforcement activities.[10]
28. The ACCC's review into data quality in the CDR found that the quality of consumer data is generally sufficient to support the delivery of CDR products and services, although improvements are required.[11] Some stakeholders noted that CDR has features that make it competitive with screen scraping, such as mandatory data sharing obligations within sectors, standardised data sharing across entities and having designated regulators to enforce data sharing requirements and protections. Some ADRs identified instances of receiving poor quality consumer data affecting the delivery of their services while others noted that data quality issues were less a concern compared to other issues such as difficulties with consent completions.[12]
29. The ACCC is working to improve data quality by increasing enforcement activities to address data quality non-compliance, providing clarification and guidance on data quality obligations, and working with stakeholders to improve processes for raising issues.
30. While progressing towards a ban, the ACCC recommends Treasury consider raising consumer awareness about the risks associated with screen scraping, and why CDR is a safer alternative. For example, it may be appropriate for consumers to be made aware of the circumstances in which they may not be entitled to recover lost funds as a result of an unauthorised transaction under the ePayments Code.[13] Increasing awareness of the CDR and its benefits, as well as the risks associated with screen scraping, will help promote CDR as a preferred alternative, increasing uptake of CDR in sectors where it is available and reducing the impact on consumers and businesses once a ban on screen scraping commences.

---

9 See CDR performance dashboard.

10 See ACCC/OAIC Compliance and Enforcement Policy for the Consumer Data Right, October 2023.

11 ACCC, *Data Quality in the Consumer Data Right: Findings from Stakeholder Consultation*, 5 April 2023, page 4.

12 ACCC, *Data Quality in the Consumer Data Right: Findings from Stakeholder Consultation*, 5 April 2023, page 6.

13 See ASIC, *Review of the ePayments Code: Further consultation*, May 2021, pp. 35-36.