Australian Government

Office of the Australian Information Commissioner

# Screen scraping – policy and regulatory implications discussion paper

Submission by the Office of the Australian Information Commissioner

Angelene Falk

Australian Information Commissioner and Privacy Commissioner

27 October 2023

OAIC

# Introduction

The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to comment on the screen scraping – policy and regulatory implications discussion paper (discussion paper). The discussion paper seeks feedback on screen scraping practices that involve consumers sharing their login details with third parties, who use those details to collect point-in-time information to provide a service to the consumer.

The OAIC supports the Government's commitment to consult on policy options to develop targeted regulation for screen scraping.[1] Screen scraping practices pose significant privacy and security risks to individuals. The OAIC has previously recommended that the Government consider prohibiting screen scraping and other unsafe online practices where safer alternatives are available.[2]

This submission expands on the privacy and security risks of screen scraping practices that involve consumers sharing their login details with third parties to allow the third party to access the consumer's personal information. We confirm our recommendation that screen scraping should be prohibited and that further consideration be given to the privacy obligations of unaccredited entities that collect personal information through the CDR, to ensure the CDR is a mature and effective alternative for sharing personal information.

# Privacy risks of screen scraping

Screen scraping practices can result in significant harm to individuals' privacy and security. When a consumer agrees to let a third party access their information through screen scraping, they are required to provide login details such as their username and password. This enables the third party to access the consumer's account to see and collect data (referred to in the paper as 'read access') and in some cases, take actions on the consumer's behalf (referred to in the paper as 'write access').

As noted in the discussion paper, screen scraping presents a range of risks. These include that the consumer may have limited control over the specific data that a third party accesses using their login credentials, and that it may not be clear to the consumer that a third party has ongoing access to their account. Sharing login details is also contrary to good privacy self-management practice and Government advice.[3] Over time, regular exposure to screen scraping practices can normalise poor privacy and security practices for consumers, which may increase their susceptibility to scams.

A data breach affecting a screen scraping provider could have significant negative consequences for affected individuals. As well as login details, screen scraping providers may hold information including bank account, transaction, or superannuation information. If this combination of information is exposed in a data breach, and particularly if combined with other information about an individual, the likelihood of consumer harm is high. In the OAIC's most recent notifiable data breaches report, 76% of individuals whose data was involved in a data breach said they experienced harm as a

[1] Response to recommendation 2.1, Government statement in response to the Statutory Review.

[2] See OAIC submission to the Statutory Review of the Consumer Data Right (CDR), recommendation 1. Separately, in relation to data scraping, the OAIC and 11 of its international data protection and privacy counterparts released a joint statement to address the issue of data scraping on social media platforms and other publicly accessible sites: see Global expectations of social media platforms and other sites to safeguard against unlawful data scraping | OAIC.

[3] Guidance on good privacy self-management practice is available at Tips to protect your privacy | OAIC; Online safety | OAIC.

result. Types of harm included an increase in scams or spam texts/emails, financial or credit fraud and identity theft.[4]

## Regulating screen scraping

The *Privacy Act 1988* (Privacy Act) contains protections for the personal information of individuals who engage with an APP entity, including through screen scraping.[5] While the Privacy Act creates core technology neutral protections, in some circumstances its principles-based framework needs to be supplemented with specific regulation to address high risk activities or sectors.[6] Given the privacy risks associated with screen scraping practices, the OAIC strongly supports specific regulation to prohibit screen scraping.[7]

The OAIC considers the CDR to be a safer and more secure alternative to screen scraping. The CDR has a strong privacy and security framework for businesses accredited to collect information through the CDR system (accredited persons), which includes:

1. CDR-specific privacy and security protections in the *Competition and Consumer Act 2010* and associated instruments, which include the CDR privacy safeguards and apply when an accredited person collects, uses or discloses personal information under the consumer data rules, and
2. privacy and security protections in the Privacy Act, which are intended to apply to accredited persons when CDR-specific obligations do not, including for personal information collected outside of the CDR.[8]

The discussion paper reiterates and seeks feedback related to the Government's commitment to support the maturity of the CDR as an alternative to unsafe practices, such as screen scraping. The OAIC recommends that as part of this work, Treasury considers CDR privacy settings to ensure overall protections remain proportionate to current and emerging risks. We recommend this include thorough consideration of the privacy obligations of unaccredited entities that collect personal information through the CDR, noting these entities currently are not covered by the full suite of privacy obligations outlined above.[9] This will support consumer trust, confidence, and engagement with the CDR in the long-term and contribute to the CDR being a sustainable ongoing alternative to screen scraping.

---

[4] Notifiable Data Breaches Report: January to June 2023 | OAIC: 76% of those whose data was involved in a breach said they experienced harm as a result. More than half (52%) reported an increase in scams or spam texts or emails. Three in ten (29%) said they had to replace key identity documents, such as a driver's licence or passport. Around 1 in 10 said they experienced significant issues such as emotional or psychological harm (12%), financial or credit fraud (11%) or identity theft (10%).

[5] Under the Privacy Act, APP entities have obligations related to their handling of personal information, including any personal information collected through screen scraping. An APP entity is defined in the Privacy Act as an agency or organisation. Small business operators are generally exempted from the definition of 'organisation' and therefore are not usually subject to the requirements in the Privacy Act. See Rights and responsibilities and APP guidelines.

[6] See OAIC submission to the Privacy Act Review Issues Paper: Part 6.

[7] See OAIC submission to the Statutory Review of the Consumer Data Right | OAIC.

[8] To avoid duplication, where a privacy safeguard applies to an accredited person the corresponding APP usually does not (except APP1 and Privacy Safeguard 1): subs 56EC(4), Competition and Consumer Act.

[9] Since May 2020, the Information Commissioner has recommended that all entities that collect personal information through the CDR should be subject to the Privacy Act, including unaccredited entities that are small business operators.