

cto / Screen Scraping in Banking

Australian Federal Treasury has just released a discussion paper that dives into the use of screen scraping to access consumer banking data.

The paper is a call to action for insights on how to best regulate this practice, especially within the banking sector.

The paper seeks to examine the current state of screen scraping, its risks, and how upcoming reforms like Open Banking could shape its future. Key questions are posed: Is the CDR a viable alternative right now? Should screen scraping be banned where CDR can be implemented?

Screen scraping involves consumers sharing login details with third parties to access accounts and collect data. This raises cybersecurity and consumer protection concerns.

Various reviews have recommended regulating screen scraping as an unsafe practice, including banning it where the Consumer Data Right (CDR) is a viable alternative. This paper consults on policy options.

How screen scraping is used

Mainly used to access banking data for services like lending assessments, financial management apps, accounting software. Also used for identity verification.

Data may be accessed as a one-off or ongoing. Consumers may not always realise scraping accesses all their data or enables ongoing access.

Risks of screen scraping

Counters cybersecurity advice not to share passwords. More parties hold login details, increasing security risks.

Banks try to block scraping which accesses accounts against terms of use. Multifactor authentication also interrupts scraping.

Limited specific regulation of scraping practices and handling of data collected. Consumers may not understand risks.

Risk of mass exposure of banking logins if a screen scraper is breached.

Consumers may lose protections under the ePayments Code if they share login details.

Reforms and reviews

Privacy Act review proposed stronger 'fair and reasonable' handling of data and Privacy Impact Assessments.

Reforms to apply responsible lending to BNPL may increase use of scraping or CDR in lending.

Government combating scams, investing in cyber security and Digital ID.

International approaches like Open Banking restrict scraping practices like impersonation.

Consumer Data Right

Safer alternative as doesn't require sharing logins. Has protections around consent, data use, deletion.

Stakeholders raise CDR has higher costs, data quality issues, complex

consents limiting uptake vs scraping.

Government working on CDR functionality - business use, consent simplification, data quality.

Open questions

How should comparability of CDR and scraping be assessed? What restricts transition to CDR?

Should scraping be banned where CDR is a viable alternative? What transition period needed?

Newer

Older

Friday, 23rd February 2024

Consumer Focus

Friday, 23rd February 2024

Navigating the Journey from Ide...

Jins © 2022-2025

Tags [RSS feed](#)

Made with [Montaigne](#) and [bigmission](#) 