October 20, 2023

Adatree Response to Screen Scraping

About Adatree:

Adatree is an Australian financial technology company at the forefront of the Consumer Data Right (CDR). As Australia's first CDR intermediary, it uses a sophisticated and secure proprietary platform to access business and consumer data from every available data source in all industries, including banking and energy. Its customers are a wide array of businesses, including more than 20 banks, credit unions, comparison websites such as iSelect, and financial services, to access consumer banking data to improve their products and services.

Adatree was cofounded by former Tyro Payments and Volt Bank employees, Jill Berry and Shane Doolan in 2019. It has won multiple technology and leadership awards, including Best Open Banking Provider and Emerging Leader of the Year at the Finnies and the Australian Fintech Awards, as well as being a national finalist in the Telstra Best of Business Awards 2022.

Overall Response:

The really key questions pertinent to the decision to ban ('regulate') screen scraping aren't asked in this paper, not even in a neutral way.

Our response will start with the questions and answers that are key, that are hard-hitting and really should make a difference in the decision about the future of the pervasive and unacceptable practice that is screen scraping. Below this, there are the questions asked in the consultation paper.

Overall, the companies facilitating screen scraping have no incentive to share comprehensive information for this consultation paper or change their business model to get rid of screen scraping. Most of the screen scraping clients would not be able to be accredited (or meet the requirements of a Representative) now without major work - this is our experience when we discuss CDR with screen scraping clients.

Hundreds of companies that engage in screen scraping are interested in the CDR and continue to screen scrape, without actively transitioning. Why? What is holding them back?

- Fundamental change in retained data - their processes retain data in many systems. The definition of CDR data and retention policies don't work with how they currently manage data.
- Derived data - they need to keep derived data
- Infosec uplift - often they wouldn't meet the technical and security obligations of the CDR regime
- Misinformation about quality / availability of CDR - screen scrapers and others without CDR data access say screen scraping is better
- Other non-CDR data sources - they want one mean for all industries
- Monetising data - they monetise scraped data with no guardrails. For this to happen in CDR, they'd need de-identification consent and disclosure to monetise data.
- Status quo - they aren't forced to uplift their security and consumer protections. They are expecting it one day and won't change until they have to

P: 02 8005 1826
W: adatree.com.au
A: Suite 1408, 3 Spring St, Sydney

What needs to be done from a technical perspective to ban screen scraping / make CDR viable?

- Mandating and enforcement of Data Holder authorisation screens (text, process, etc)
- Mandate Data Holder SLAs for response and resolutions with fines for not meeting them
- Mandate Data Holder uptime reporting publicly
- Streamline the processes to create and public software products on the register
- Standardise what is shown in consent screens and what register fields are displayed, specifically for CDR Representatives

What needs to be done from a regulatory perspective to ban screen scraping / make CDR viable?

- Changing of definition of CDR Data
- Removal of derived data
- Make insights principal based, not prescriptive (see operational enhancements response paper)
- Allowing some types / amounts of data to be kept for certain purposes - align to the UK
- Introduce legislation where consumers are told when their data is sold and they have the option to decline it
- Proactive and regular enforcement of PS11
- Strong enforcement of CDR Principals
- Introduce trial CDR limit of 100 consumers so parties can trial CDR in production (beta users)

What needs to be done from a consumer perspective to ban screen scraping / make CDR viable?

- Communication / education campaigns about dangers of screen scraping and about CDR. Specifically:
    - Inform them there is a change and what to expect.
    - Inform them what you can trust and what you can't.

Formal consultation paper - Adatree responses:

1. What screen scraping practices are you aware of or involved in?

Adatree is aware of screen scraping for primarily banking data. The main screen scrapers in Australia are Yodlee, Basiq, Credit Sense, and illion (the service formerly known as BankStatements.com). It is sometimes called digital data capture.

Adatree is not involved in any screen scraping (unregulated) data practices.

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?

The main intent of screen scrapers of which Adatree engages in discussions about (comparing screen scraping to CDR) retrieves banking data through the screen scraper to give to the screen scraper's client (e.g. a non-bank lender or PFM).

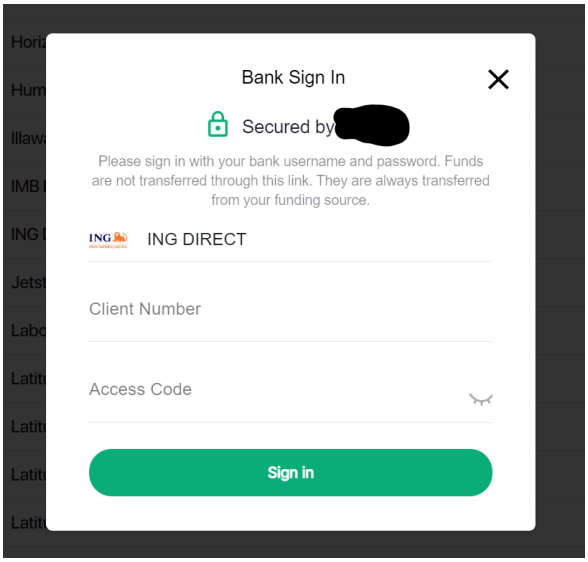
Banking data is commonly captured, but other sources include superannuation, non-bank lending, government data (MyGov) and insurance.

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?

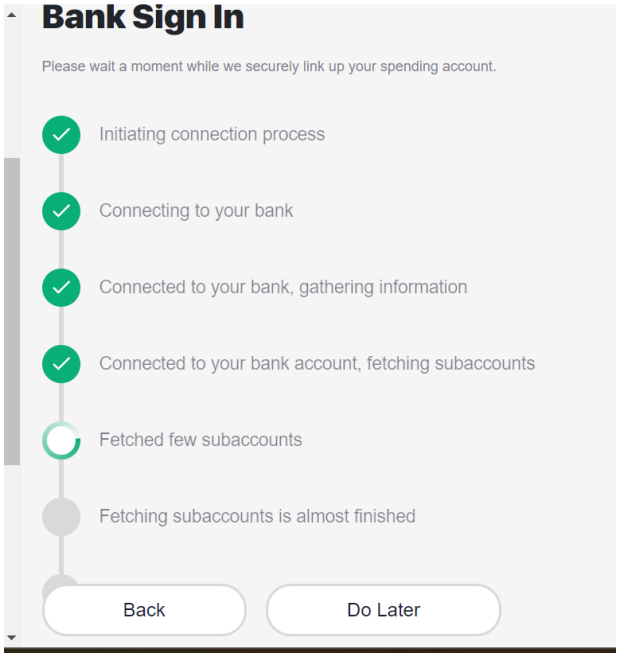
Here are screenshots of a screen scraping process. The (anonymised) provider has done this for > 300,000 Australians.

Starting from clicking 'Connect <name of product> account':

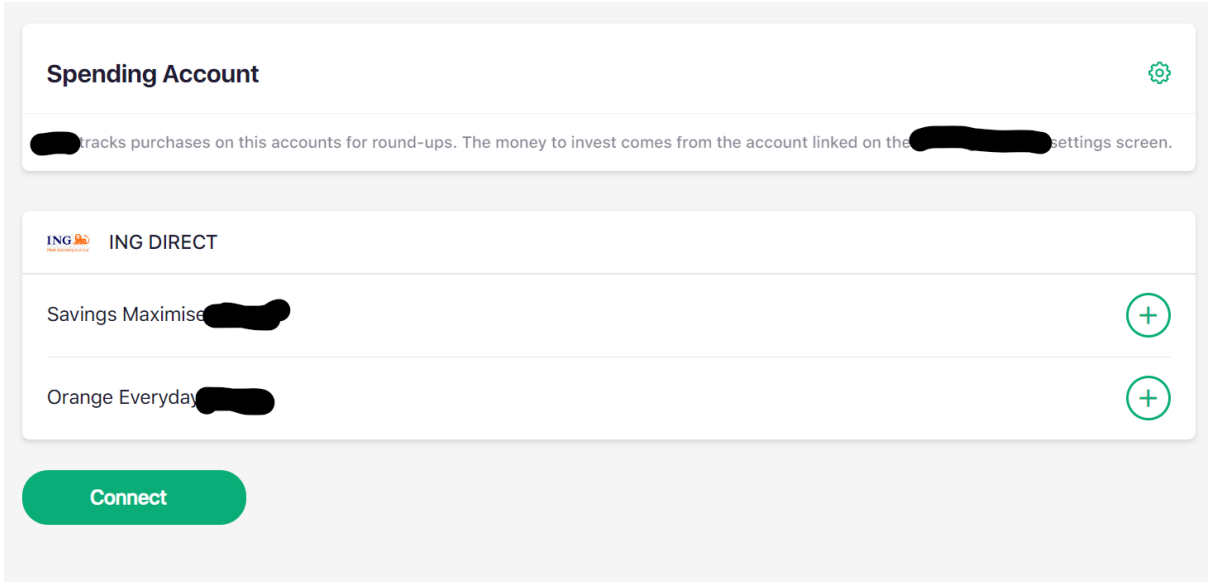
Sign in page - no disclaimer about who they use, what they collect. They ask for bank login information, carte blanche.



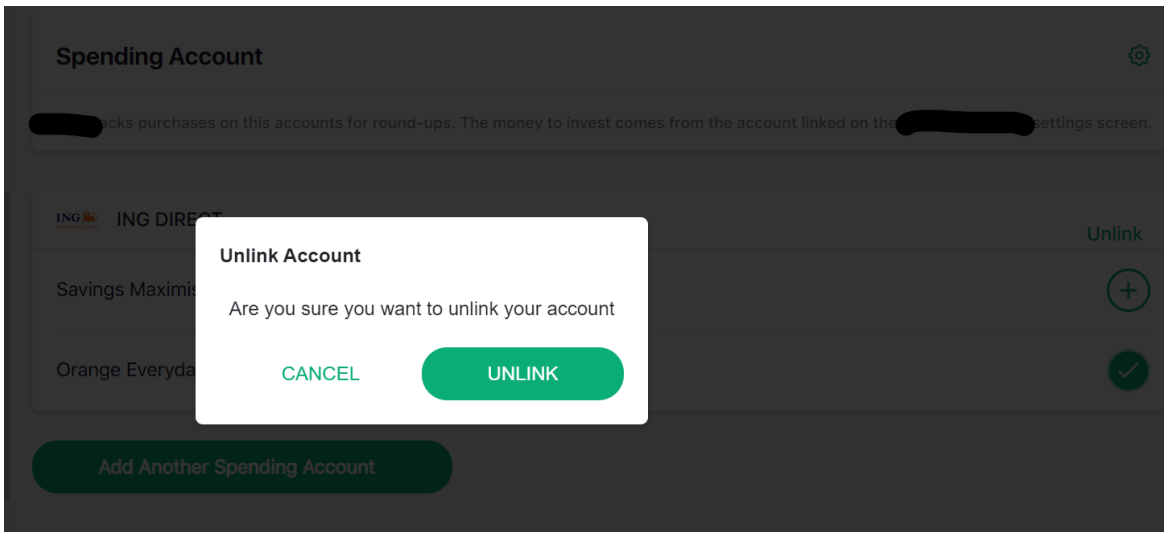
Connecting status page after giving password



Select account(s). (No terms)



Deep in settings - can choose the funding account and click ‘delink’. This is the confirmation page.



What isn't included in this process:

- **Disclosure** - The only information is "you agree and acknowledge that you must use the App to connect your <fintech account name> to your <fintech account name> to make investments;
- **Storage of data / Data treatment** - No information. about deletion, storage of raw, derived data
- **Third parties** - who do they use?
- **Location** - Where is the data stored? (them and their third parties)
- **Protections** - IT security controls
- **Selling Data** - This company in the screen shots monetises their users' screen scraped data. Neither in the terms nor the scraping process does it say that.
- **Limitation on types of data -** It is assumed that they collect all data, far more than what they need
- **Frequency** - no timing or information about how often data is collected
- **How to stop sharing** - No information given. Deep in settings, you can unlink, if you search for it.
- **What happens if sharing is stopped:** No information given about continuity of service
- **Option to delete -** None
- **Option to de-identify** - none
- **Non-screen scraping alternative -** Screen scraping is the only way to activate this core product feature.
- **Confirmation** - none

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?

Consumers don't have the choice to share screen scraped data as a one-off or choose the term of data access. There are no obligations about telling them of ongoing access. They

can only guaranteed cancelling a sharing arrangement by changing their password. It is unclear whether scrapers require the implementation of a ‘delink’ button or the rules around it. How many millions of Australians have shared data, failed to cancel, and have their data harvested and sold unknowingly?

From the above example, there is neither information (in the terms, as linked), nor in the consent process about the duration of access, frequency of data access or how to cancel. This provider does have it in their app FAQ guide if you search for it.

While it is easy to connect an account, there is no information provided past that.

In 2021, we were emailing with a journalist about how a fintech was asking him for his password (screen scraping), and the nuances of that process. That fintech is now defunct. This raises further questions, like - the consumer never delinked their account, the fintech assumedly doesn’t have access, but is the screen scraper still collecting and selling the consumer’s information? They still have the username and password, and unless they’ve changed their banking username and password, it is truly unknown. How would they know who is accessing their account? Especially when the third party provider is never disclosed - there is no one to ask.

d) Do you use screen scraping for purposes other than data collection (for example to undertake actions on behalf of a customer)?

We do not know of any companies using screen scraping for actions.

2. Are there any other risks to consumers from sharing their login details through screen scraping?

As touched on in the consultation paper, there are two main risks: the aggregated risk of Australians having just shared their username and password indefinitely with parties (that they don’t know), and they have breached their account terms.

1 - Screen scrapers as a honeypot.

As per the screenshots in 1b, the process and terms do not show the consumer who the underlying screen scraper is. Screen scrapers store the bank account login details (username & password) of millions of Australians, in an unregulated data environment.

Given the loss to Australians with so many public cybersecurity hacks and breaches of Australian companies, it surely is only a matter of time before these screen scrapers are targeted and successfully hacked. This would introduce an incredibly high liability and harm to Australians given the breach of their bank account terms and conditions (below).

In 2020, a representative from ASIC said that, “there's no evidence of which we're aware of any consumer loss from screen scraping.” This attitude is no longer acceptable - there is a

huge risk to Australians by allowing this unacceptable behaviour to exist. It is not a question of *if* there would be losses - it is only a question of *when*. The days of regulators condoning this behaviour needs to stop - especially when the three screen scrapers could make a market-driven decision to migrate to CDR. They have not, and legislative action is urgently needed to drive regulatory-driven change. Regulations are changing after the major breaches of Australian sensitive information. Changes are needed before there is incredible loss to Australians on a major scale.

2 - Breach of Bank Account Terms - As NAB says, “Giving your NAB Internet Banking password to a third-party breaches NAB's Internet Banking terms and conditions” and they could be “liable for losses caused by unauthorised transactions.”

Most ADIs have similar wording to this in their account terms and conditions. It is unacceptable to write your PIN on your debit card and leave it - you would be likely to be liable for any losses. How would this be treated any differently when sharing your password and username?

39.4 User's responsibilities under the ePayments Code

(a) Where NAB provides the user with an authentication service and/or password the user must not:

(i) voluntarily disclose the authentication service and/or password to anyone including a family member or friend, except when you are creating an authorised user;

(ii) act with extreme carelessness in failing to protect the security of the authentication service and/or password; and

(iii) record the password without making any reasonable attempt to protect the security of the password record on the one article or on several articles so that they are liable to loss or theft simultaneously.

(b) Where NAB allows the user to select a password or change the user's password the user must not select:

(i) a numeric code which represents the user's birth date; or

(ii) an alphabetical code, which is a recognisable part of the user's name.

Either of these selections may mean you are liable for losses caused by unauthorised transactions caused by a breach of the security of the password.

3. Do you have any data, case studies, or further information about the risks of consumers sharing their login details through screen scraping?

The only further commentary would be about the sale of Australians’ banking data by the screen scraper and/or the clients themselves, with no information shared or consented received by Australians themselves. One reason that companies are hesitant to transition to CDR is because of the income they receive selling banking data.

When Australians connect their bank accounts and share their banking login details, they assume it is for a service. Do they know it is being sold? In this unregulated data sharing

practice, there is no standard, regulated practice or oversight about the masking of data. Some companies say they 'depersonalise' it - this is not in line with the CSIRO's De-Identification Framework - and would likely not pass the requirements to de-identify data as required in the CDR Regime.

While consumer risks and harm isn't blatant with monetary losses (yet), it is about the murky and unethical practices happening that neither regulators nor consumers are remotely aware of. This is against all principles of the CDR and why regulated data sharing frameworks have been introduced worldwide.

Screen scraping is beyond regulation or reform. It needs to be banned to end these non-consented, uninformed practices.

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?

None.

If anything, this shows that screen scraping is unreliable as it is subject to an organisation's front end being static and not having MFA. It would have much more downtime than CDR's data source availability.

5. Could you provide any examples of how your organisation or entities you partner with manage the risks associated with screen scraping?

We have heard of the opposite - companies that sell data from screen scraping, of storing and sharing with other organisations. They capitalise on the lack of limitations and frameworks associated with screen scraped data - exploiting the risks and loopholes instead of managing them.

These details are not for public view with the consultation response, but we can discuss in the 1-1 meeting with Treasury.

6. Are there other proposed reforms or legal frameworks that relate to the use of screen scraping?

The Privacy Act reform, Digital ID Framework.

7. Are there any other international developments that should be considered?

The timing, criteria and data treatment of screen scraping banning in the UK and other countries.

8. What are your views on the comparability of screen scraping and the CDR?

This is compared in the below chart, from different POVs.

View of a screen scraper:

	Pros	Cons
Screen Scraping	● No regulation on screens or disclaimers presented ● Can sell the data without notifying the customer / consent ● Doesn't have to delete the data ● Practices aren't regulated ● Able to keep all data ● Able to scrape almost any source of password protected data	● Will be banned eventually
CDR	● Trusted logo to use ● Can be regulated as an ADR but not mandated to actually use it / ask their customers to adopt it ● Additional data sources not connected via screen scraping	● Rollout of data sources to other industries dependent on Data Holders and legislation ● They lose their income selling 'de-personalised' data

View of a consumer:

	Pros	Cons
Screen Scraping	● Faster consent process (one click)	● Unregulated ● Breaches account terms ● Likely liable for losses ● Not informed how to stop sharing - often unable to besides changing password ● No notifications that sharing is ongoing ● Can't easily stop ● No known information about the underlying supporting parties ● Data is sold without their knowledge

CDR	● Trusted regulated framework ● Consistent process consenting with organisations	● Probably hasn't heard of CDR ● Variable consumer experience with different data holders

View of a company capturing data:

	Pros	**Cons**
Screen Scraping	● No accreditation / audits needed ● No restrictions of treatment, storage or access of the data ● No barriers to entry	● Scrapers find it difficult to build connections to non-individual accounts, which limits the usefulness of the service. ● Data Holders often block it, causes unreliable downtime
CDR	● Ethical data sharing practices ● Stronger consumer protections ● Standardised data formats between every Data Holder ● Strong NFRs for peak and non-peak ● Data Holders actively engaged if any issues ● Data Holders don't block this	● Nominated representative processes exist and are not standardised ● Challenging to delete data and navigate retaining it ● No ability to trial in beta - all protections must be in place

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?

What can't be accessed through screen scraping:

- Extensive metadata not shown in online banking
- Longevity of up to 7 years (instead of normal 90 days of screen scraping)
- Closed accounts
- All products
- All Data Holders

What can't be accessed through CDR:

- Downloaded PDF statements
- Access to data / organisations that are not yet live in CDR (e.g. super, insurance, MyGov)

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?

There are major reasons that companies choose to use screen scraping - largely that relate to the treatment of data:

- They can keep the data and embed in their systems
- They can share the data with third parties, indefinitely
- They can sell the data
- Data retention isn't subject to the DDF
- Their data models / credit models can learn from the screen scraped data (derived data)
- The consent process is 'easier' than CDR (note: no consumer disclaimers, protections, choices, etc)
- There is no POC or way to trial CDR - the protections start at the first consent

In short - the major restriction is the defined terms in the Rules of 'CDR Data', especially including 'derived data'.

d) Can you provide suggestions on how the CDR framework could be adjusted so that it is a more viable alternative to screen scraping?

There are major issues with the CDR regulatory framework. That affects the viability of the CDR as an alternative to screen scraping. **The definition of CDR data and derived data are really key ones and must be changed.** It essentially treats data like kryptonite. Wherever that data goes, you have to have a CDR data boundary around it. That boundary doesn't happen like this in other countries and it definitely doesn't happen with screen scraping. In scraping and in the UK, you can keep the data wherever, you can sell it, you can put it in any systems - there are no restrictions on what you do with it.

When looking at the banning of screen scraping and transitioning into the CDR, businesses are looking at not only the convenience and choice afforded by the CDR, but more importantly for them, how they have to deal with the data. CDR regulations have introduced new ways how to work with the data inside and outside of CDR, like TAs. With trusted advisors, they can leverage people's existing licensing and accreditations so they can use the data within their existing arrangements and systems. Also with business consumer disclosure consents, you can actually give data to specified persons (if you're not an individual). These are essentially off-ramps for the CDR and makes the data much more usable for the companies that are trying to leverage this data.There's the issues of the nominated representatives for business accounts, but with the improved raised in the concurrent operational enhancements paper, that will no longer be an issue.

So the big question is the definition of CDR data and derived data. Privacy and utility really need to be balanced with CDR data. It is swinging too far towards privacy right now so that it's challenging to be usable, solely because of these definitions in the CDR Rules.

It is so challenging for businesses to even leverage this data if they totally have to delete it. One example is there's a lot of companies that use aggregated data to create and improve their data models through machine learning. if a consumer has the right to deletion, and that is deleted out of the pool. then they would essentially have to just constantly tear down and build back up their models every time there is a deletion request. This is a major inhibitor to CDR and has nothing to do with technical availability - only defined terms in the Rules.

It doesn't work with how businesses actually leverage data right now. If you get a customer's name and address through CDR data, and put it in the CRM - that has to be deleted in Australia. In the UK, you could use and keep that data still, even after consent has expired.Ultimately, data needs to be stored to make algorithms smarter, which leads to better consumer outcomes.

It doesn't work like that in the CDR and there's been hundreds of companies that have been interested in the CDR. So if the motivation, if the project planning and budgets are there, then what's actually holding them back?

One issue is trialing in production. Some companies we speak to would like to have a beta period in production; however, they need to have all controls and assessments in place even just for one consent. An idea would be to introduce a trial period for a maximum of 100 consumers to consent without the checks being complete. The UI could be changed to notify the consumer, who would likely be an internal staff member trialing the process, that the full audit / checks haven't been in place. When there is a full rollout and go to market, the full checks must be in place by the regulator and/or the CDR Principal. It is rumoured that some CDR principals currently do this already, so this should either be allowed or explicitly banned, so it is an even playing field.

If Australia were to mimic the data protections of the UK, it would introduce more of an off-ramp of what you can do with the data. There should be protections in place, e.g. disclaimers that it can't be sold without approvals, that bare minimum information could be stored for customer identifier purposes, but not full transaction datasets, that are attributable directly to a consumer. Consumers would have some rights to deletion but maybe only certain types of data must always to be deleted, and that they can keep it for customer record keeping or the like. The current requirements to delete all and have identifiers all throughout all of your systems that make it pretty challenging. It could be easily principle based about what data recipients (or Reps) could retain and why.

There are new ways to work with data within and outside of the CDR, including trusted advisers (leveraging their existing accreditations, licensing and certifications and letting them use the data within their existing arrangements) and business consumer disclosure consents (BCDC) to give data to 'specified persons'.

Examples of how current rules don't work with use cases:

1 - Banking Energy

One common banking data use case is looking for a more competitive home loan. You can look for a rate and unfortunately if you want to switch to a new bank, you have to enter all of this information in again, if the bank isn't an ADR or Rep. This is if the consumer went directly to the new bank.

However, if the consumer went to a mortgage broker, which is a TA, they can then share that data on to banks, as they currently do in performing their business.

If there's the same end bank, but one route is direct and one is through a broker, there are two polarising treatments of data and requirements to receive and retain it. This is unacceptable. The negative nuances of the law are preventing companies from receiving CDR data - and making Australians worse off in the process. This is the consumer harm realised from the current definition of CDR data.

Changing the rule about CDR data would fix this.

2 - Switching from Electricity to Solar - using Energy Data

A use case for energy data looks at a consumer's electricity usage, including peaks and troughs, so a company can recommend appropriate solar panels and/or batteries for the consumer based on their actual usage.

If they did the analysis on CDR (energy) data, there would be an answer of 'Claire should get solar panels sized XYZ'. That XYZ is considered derived data. That means if an ADR or Rep were to disclose that to a solar installer, that is a breach of the law since derived (CDR) data is leaving the CDR ecosystem. Claire will clearly tell the solar installer her address to install it, and again, sharing her address collected through the CDR would also be considered a second breach.

The way that you could share the information while being compliant is by making Claire retype her recommendations and address to the installer. This is a major nuisance to Claire, is unnecessary busywork and she was always going to share this information. The only consumer harm here is that it is introducing unnecessary friction. Clarie is no better off and this wonderful use case is not implemented, and Aussies like Claire stay on electricity. There are no TAs in energy which doesn't help the situation.

Changing the rule about CDR data would fix this.

Government Options going forward.

Assuming there is a ban in place for industries where CDR is an alternative, the government has a few main options for fixing this and having an immediate increase in adoption:

- **Helping uplift companies' infosec capabilities needing to store data -** If screen scraping will be banned, most companies would need major policy, controls and process uplifts. Screen scraping is the lowest common denominator where there are no required security measures, which is unacceptable. The CDR ones are challenging now. If these security measures (Schedule 2) need to be upheld, then there should be a government-funded program to help all companies accessing data increase their security postures. Screen scraping has no barriers, so introducing very high ones also won't work. Either help them reach the barriers, or lower them a bit.
- **Extending BCDC treatment to consumers -** non-individuals can share their data (through an ADR) with 'specified persons'. This isn't CDR data anymore and the protections of data no longer apply. If this stance is considered acceptable and appropriate by the regulators, how is this
- **Change the definition of CDR Data -** remove derived data, allow some data to be kept by default for certain administrative purposes (e.g. CRM record keeping).
- Immediately implement the recommendations from the **Operational Enhancements** paper.
- **Proactive enforcement of Privacy Safeguard 11:** In lieu of a complete and comprehensive CTS for DHs, the ACCC and OAIC need to proactively ask all Data Holders for evidence of how they are meeting PS11. Many Data Holders aren't actually testing the quality of data they are sharing. There are tools (like Adatree's) in market to assure them of this. This would fix the Data Quality issue for the regulator to be proactively and regularly checking the Data Holders quality processes and meeting of obligations.
- **Very strong enforcement of CDR Principals -** With increased CDR participation, it is only as good as the weakest list. For some CDR Principals that ask for minimal information and would seem to flout the CDR rules for their representatives, this is the biggest threat. Regulators must actively and regularly discuss the assessment (initial and ongoing) criteria Principals use.
- **Streamlined processes** for technical engagement with the ACCC Registry (e.g. tickets, registration of software products)
- Make **industry rollouts faster**.
- Introduce a **trial period for CDR production**

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?

The government needs to consider the following:

- Success metrics (creating and measuring them)
- Timelines of implementing operational enhancements
- Discuss with formerly aspiring ADRs / Reps why they didn't go through with the CDR switch. Do deep root causes analyses.
- Availability of data sources
- Maturity of data sources

- Consumer protections - oblivious to the harm on millions of Australians where their data is unknowingly harvested and sold now
- Price of compliance vs non-compliance with CDR (e.g. ING fine amount) and increasing infringements
- Introducing an ability to trial CDR data

The government needs to start consenting themselves. As has been raised in DSAC for years, success metrics are needed to quantifiably say that something is ready or not based on fact, not just on opinion.

We don't think the issue is the technical readiness, data sources, availability or data quality of the CDR. These are good now, and especially with the very practical recommendations in the Operational Enhancements paper will only improve.

CDR is at a point now - it is better than it was, and it will only get better. A line in the sand needs to be drawn not based on where it is now, but where it will be at the point of screen scraping.

Also, when considering views, think of:

- Motivations of people who are making those statements. For example, people at organisations with no CDR Access or screen scrapers love to say the data quality isn't there. However, Adatree is the only company connected to every data source. How would they know about the industry-wide data sources? Where is their evidence?
- The state of CDR in 12 months when the operational enhancements will be live.

b) What are your views on a ban on screen scraping where the CDR is a viable alternative?

Adatree vehemently supports the ban on screen scraping. There will be excuses left and right about why screen scraping for banking data needs to be allowed. The imminent potential for damage is rampant. It is far beyond rectifying screen scraping given the lack of processes, security controls and major hidden pitfalls for consumers.

With the regulatory changes mentioned in 8, this will make it very viable for **all** businesses to migrate from screen scraping to the CDR. If screen scraping is regulated, the CDR will be a failure and it should've just been done back in 2017. It must be banned. Other countries have done it. The UK has strong adoption because of their less strict data protections but also a strong mandate in place.

Because screen scrapers are connected to, collecting and on-selling data of millions of Australians, the government must mandate that:

- screen scrapers immediately stop selling banking data
- Disconnect and stop scraping data from accounts where the consumer hasn't actively been logged in to the service for 3 months

- Notify every consumer that their bank accounts are actively having data collected and on-sold
- Introduce immediate required disclosures for every industry where their data is collected and sold
- These above steps must be done by screen scrapers as a condition to keep their CDR accreditation. They are currently having the benefits of branding as a regulated company, but they continue their unregulated and unethical data collection practices.
- No new companies are allowed to participate in screen scraping (no new customers)

With billions invested into CDR across all participants, this is the time for the government to back its own initiative.

c) What timeframe would be required for an industry transition away from screen scraping and why?

This needs to be announced that it will be banned as soon as possible. Even for the ban, there can be no new companies that don't already use screen scraping to meet their responsible lending obligations. No new onboarding - this is only focused on off-boarding.

Another way to do this is that for screen scrapers that are also ADRs, their licensing should be suspended if they are offering both services for industries already live. They need to be be on Team CDR or off of it.

There should be a consultation to reprioritise industries based on what is scraped now, and that should influence the concurrent rollout to other designated industries.

With the aforementioned technical, consumer and regulatory changes were in place, it could change very quickly. A **very reasonable timeframe** would be a ban on live industries (e.g. banking and energy) by 1 February 2025 for banking data. It isn't just a timeline but all of the other changes in legislation, CDR standards, CX guidelines and operational processes to accompany it. Nominated representatives changing (all being automatically opted in) and changing authentication measures must happen as a priority.

Ongoing for other industries, it should be banned 12 months after CDR goes live for that industry. This also means that Data Holders should not have exemptions for delays and have to immediately start to share data of high quality and uptime.

Things are moving quickly in digital identity and other cybersecurity protections after the breaches. The CDR regulators and regulators that would ban screen scraping need to act with haste as if this has happened.

CDR is currently more reliable, more widespread with sources and has more coverage over products and of course metadata. It is safer for consumers.

Timing of other regulatory obligations needs to be considered, e.g. NBL & NBPL have CDR & responsible lending obligations. They have to meet their responsible lending obligations - they shouldn't be allowed to do so with screen scraping; It must be through CDR. There's no point in introducing that obligation where they use a dying access method that will be banned inevitably. Screen scraping must be grandfathered before it is totally banned, like a bank having a product open but not allowing new applications.