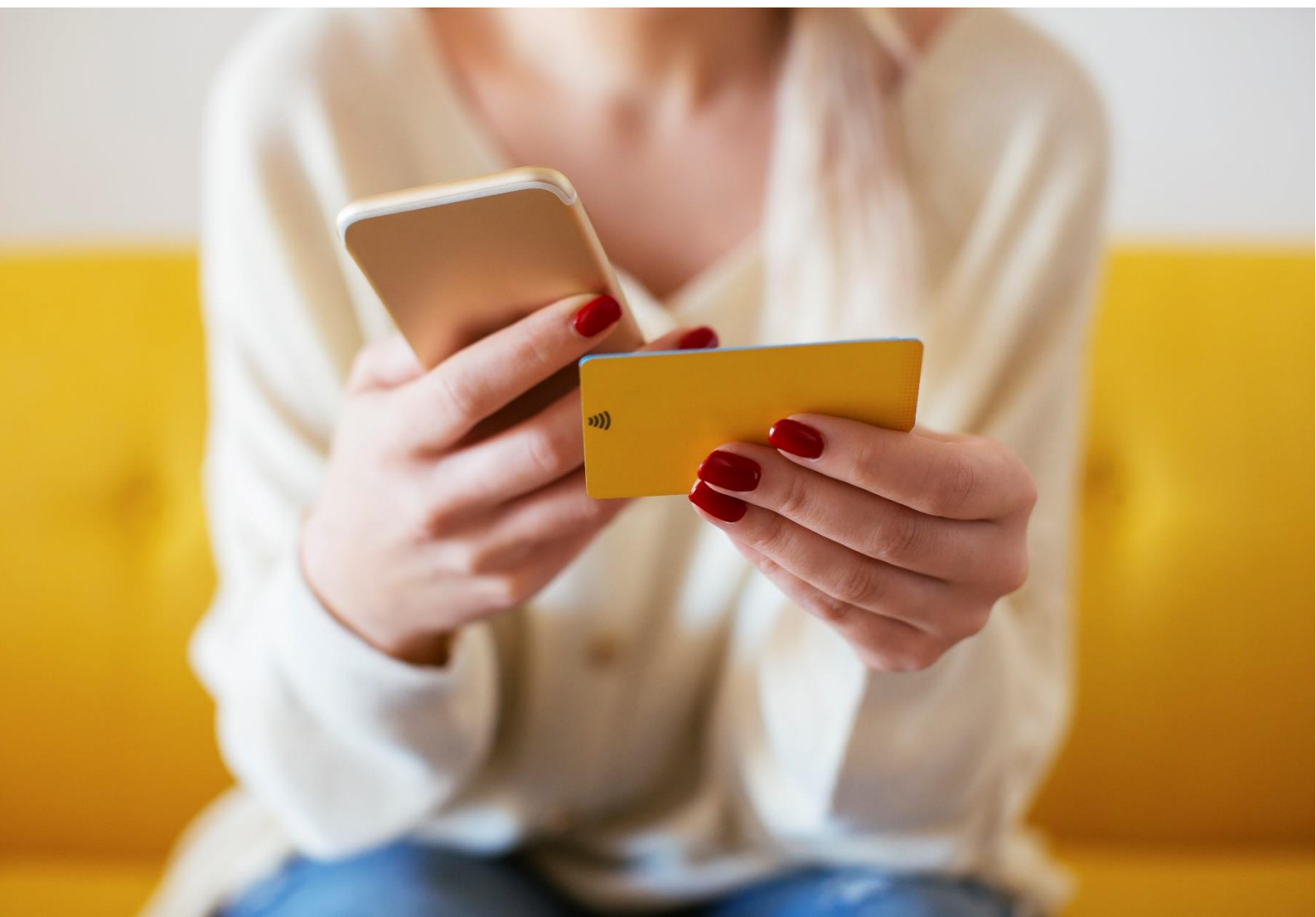


Mapping dispute resolution on digital platforms



accenture

Table of Contents

Executive summary	2
Introduction	4
Approach	5
Glossary	7
1. Diversity of the landscape	8
2. Context of issues.....	15
3. Advantages and challenges	18
4. Mapping dispute resolution	21
5. Pain points	34
6. Potential opportunities.....	50

Executive summary

The range of issues, complaints and disputes on digital platforms is a diverse problem

Digital platforms are increasingly part of our lives and businesses, with 80% of individuals using social media and 50% of businesses with an online presence.¹ This results in a number of issues, challenges and disputes given the scale and scope of interactions now undertaken online.

Each year the platforms included in the study² address a range of issues, complaints and disputes in Australia, which can range from high volume customer service interactions like spam, management of accounts and payments to more subjective and complex complaints like fake reviews, transparency of ad performance, hacking and scams.³ These issues vary depending on the platform, its users and its service offering.

Many of the challenges are not new

Many of the issues and challenges faced online are not new. For example, 50% of scams are still undertaken over the phone.⁴

There are several existing regulatory bodies and ombudsmen in place to address some of these issues. However, addressing these issues in a digital context can amplify the problem and provides some new challenges given the ‘multi-sided’ nature of platforms and the volume of global user driven activity.

The current dispute system prevents or resolves most potential problems from escalating, however, there are 2.4 million complaints on digital platforms each year

Platforms have put in place a range of sophisticated capabilities to prevent and minimise approximately 75 million potential problems each year in Australia before they escalate. Machine learning, AI and specialist review teams work proactively to block harmful content, eliminate bad actors and scams, demote or remove fake reviews and enforce guidelines.

These capabilities enable platforms to prevent 95% of potential problems before they were experienced by the user, or result in a complaint or dispute. In 2020, this resulted in the following issues, complaints and disputes experienced on digital platforms:

- 4.2 million issues experienced, which included complaints and disputes but also issues that were resolved by users without complaining to a platform
- 2.4 million complaints to platforms
- 880,000 internal disputes, where users may have disagreed with a platform’s decision and sought a different outcome
- 190,000 external disputes where users utilised external bodies like the ACCC, state-based consumer affairs or the small business ombudsman to resolve their dispute

The most commonly experienced issues were scams, hacking and fake accounts.

¹ ABS, [Retail Trade Australia, April 2021 – Online sales](#); We are social/Hootsuite [Digital 2021 – Australia report](#)

² These included search engines, social media, payments, entertainment and media, marketplaces, ridesharing, delivery and dating applications

³ Accenture Consumer and Business Survey

⁴ ACCC [Scamwatch](#)

Complaints and issues that are addressed by users within the platform are resolved much faster and with higher satisfaction, compared to those that involved disputes and external escalation.

There are several challenges which result in pain points for businesses and consumers

There are several challenges within the system that result in approximately 880,000 disputes each year. In addition, 16% of issues on digital platforms remain unresolved. Key pain points include:

- Handling the immense scale and scope of issues requires automated and scalable capabilities which means it is difficult to tailor responses for more complex cases.
- There is a lot of misdirection for consumers that cannot resolve their complaint within the platform. Navigating external escalation is complex and can involve durations of 2-3 months through contacting and re-telling issues to multiple agencies.
- Providing transparency can be difficult as it can also lead to gaming of the system and sabotaging effectiveness of existing risk management processes. However, surveys and interviews with users show that in some cases, basic information about why their content had been blocked or account removed was very difficult to obtain.

Given the scale and scope of interactions online, the economic cost of issues, complaints and disputes in Australia each year is \$4.2 billion. Of which the majority (\$3.7 billion) is the cost to users and businesses. A significant driver of this cost is the time and effort associated with misdirection and difficulties in resolution when an issue or complaint escalates to a dispute.

s47C - deliberative processes

Introduction

The purpose of this document is to map the current dispute resolution landscape

The growth of the digital economy comes with new challenges

Digital platforms have transformed society, economies and culture globally through easily accessible information, new ways to connect with friends and family, as well as increased opportunities to participate in global trade. These trends have been amplified through COVID as social distancing measures required many people to work, connect and purchase goods and services online. For example, online sales in Australia have grown at 28% per annum on average between 2013 and 2020, jumping more than \$1 billion through COVID.⁵ In addition, social media is becoming increasingly ubiquitous with many major platforms reaching 50-80% penetration amongst internet users.⁶

The digitisation of the economy has led to a range of consumer benefits and productivity enhancing outcomes. However, the shift has resulted in some risks to consumers and businesses. Based on complaints received by the ACCC between 2014 and 2018, reports of scams occurring via social media and the losses incurred almost doubled. In 2020, the number of scams reported to Scamwatch via the internet and social media amounted to 23,325.⁷

The ACCC's Digital Platforms Inquiry raised concerns around growth in the false representations and scam content, facilitated by digital platforms and the effectiveness of current dispute resolution processes, particularly around the transparency of advertising products and the ability to resolve fake reviews.⁸ The Inquiry made broad recommendations about the potential need for further action by platforms and government.

DITRDC has identified a need for further understanding of dispute resolution processes

The Department identified that more information and data on the current landscape was needed to determine whether any action by government was required. There is an expansive scale and scope of issues, complaints and disputes that are managed by platforms and external agencies. However, there is currently limited evidence on the effectiveness of the dispute resolution landscape, including the key processes, volumes, capabilities and challenges.

This report provides a mapping of the current dispute resolution landscape

Accenture was engaged by DITRDC to undertake a mapping of the current dispute resolution landscape and survey businesses and individuals who had experienced issues while using the services of major digital platforms. This report was commissioned by DITRDC as an input into their External Dispute Resolution Scheme Feasibility Study. This report outlines the results of these two tasks and provides an evidence base to inform the pathway forward and whether there is a need for government intervention. The report covers the following:

- the nature of issues faced by consumers and businesses on digital platforms, and the extent to which these result in complaints and disputes;
- a mapping of the current processes;
- the differences across various issues, platforms and users; and
- some of the challenges that are experienced by users, platforms and relevant agencies.

⁵ ABS, [Retail Trade Australia, April 2021 – Online sales](#)

⁶ We are social/Hootsuite, [Digital 2021 – Australia report](#)

⁷ ACCC (2021) [Scamwatch](#)

⁸ See ACCC [Digital Platforms Inquiry Final Report 2019](#), ch 8.

Approach

During this 10-week project, Accenture developed an understanding of the current state of dispute resolution within the digital platforms landscape and mapped how it works today.

Exhibit 1 illustrates this approach, which was informed by both primary and secondary research, including:

- A survey of 3,488 consumers and businesses that had an issue, complaint or dispute on a digital platform. 9,805 consumers and SMBs were screened to determine the prevalence across the population.
- Ethnographic interviews⁹ with 18 consumers and businesses.
- Interviews with relevant government agencies and regulators
- Interviews and data from digital platforms
- Review of existing domestic and international literature and policy

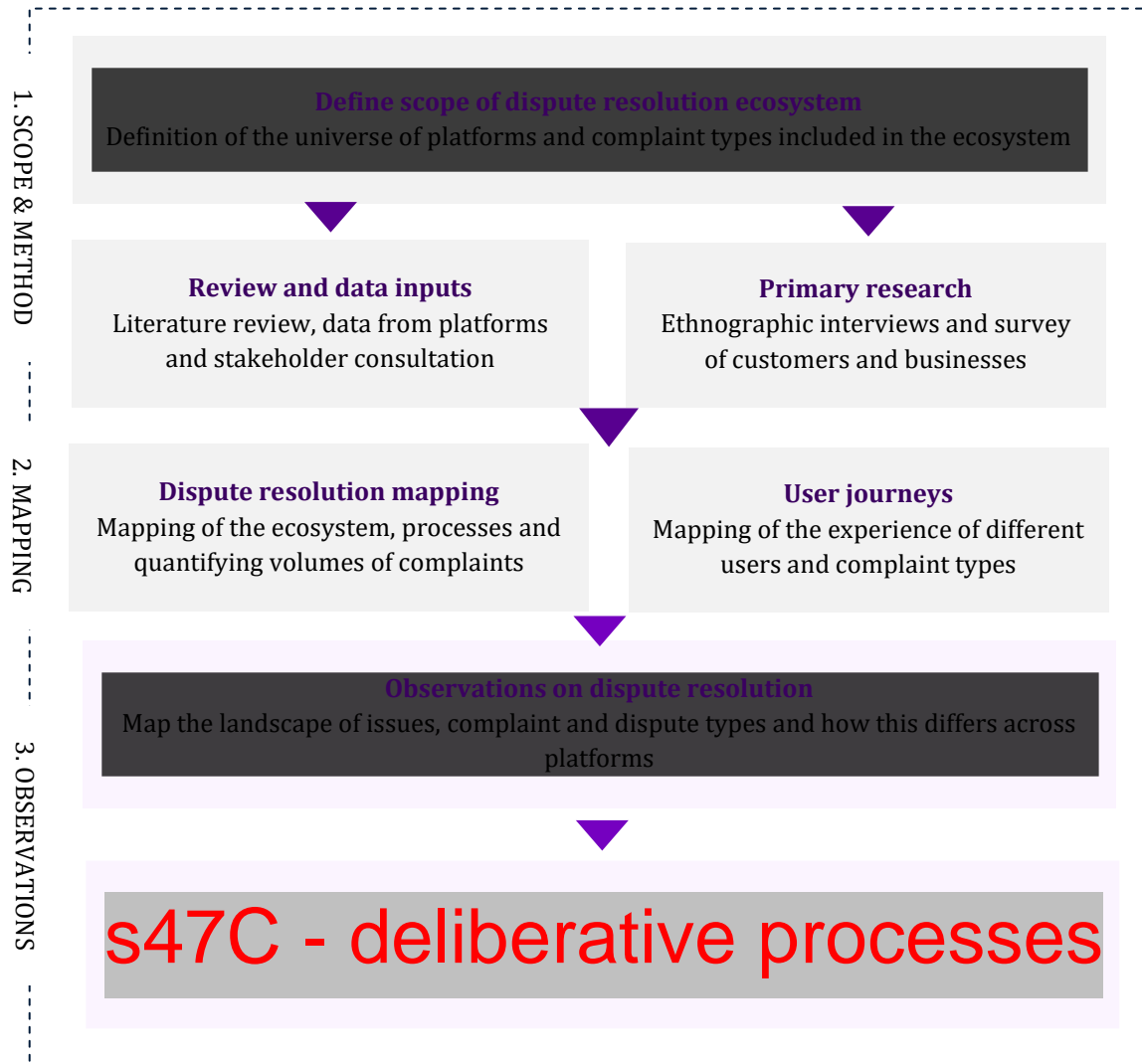
This approach was used to map the dispute resolution landscape and inform observations on how it is operating, as well as the differences across issues and platforms.

The approach required defining several situations which could occur in the process leading to a dispute. The difficulties or challenges that users experience on platforms differ in the nature of complexity. We define the following as part of this user experience:

- **Issues:** in the survey, an experienced issue is defined as a problem a user experiences on a digital platform. This could include, for example, resolving a payment issue on a platform between a buyer and seller without involving the platform. Experienced issues exclude those issues that are observed and where no action is taken. Issues exclude the prevented problems that platforms manage (e.g. through AI) before any user has been impacted.
- **Complaint:** an issue becomes a complaint to a platform when the user contacts the platform directly to resolve the issue, such as complaining about the removal of their content on a platform.
- **Internal dispute:** occurs when the platform makes a decision regarding a complaint that the user disagrees with and follows up with the platform. Examples of this can include appealing a decision or action a platform took against a user, such as a removal of an account after an initial complaint to restore the account.
- **External dispute:** occurs when the user contacts an external body to try and resolve, after attempting to resolve the dispute through the platform.¹⁰ An example of this could be a fake review that a business requests to be removed within the platform. If the business cannot get a resolution within the platform, they may dispute this through an external body like the ASBFEO. External disputes exclude issues that might be reported externally as part of a complaint or issue, which do not result in a dispute. Collectively, both external disputes and issues or complaints that involve some form of reporting or escalation to an external body are referred to as external escalation.

⁹ Ethnographic interviews are informal interviews where the goal is to learn more about the views, attitudes, behaviours and experience of members of a community in their own words and in a natural setting.

¹⁰ This figure excludes those which are reported to a third party but do not involve a dispute with the platform (264,000).

Exhibit 1**Our approach**

Glossary

Term	Description
Potential problem	Problems that are proactively prevented by platforms; platforms use machine learning, artificial intelligence, analytical algorithms and specialist review teams to detect and automatically remove potential problems before users experience them
Issue	An issue is a problem that occurs on a platform. Platforms undertake a range of preventative activities to resolve a vast majority of issues swiftly before any user is impacted.
Experienced issue	An issue experienced by a user on a platform, and where some action is taken to resolve or respond to it. These are issues that are more difficult for platforms to proactively identify and prevent at the outset, and therefore end up impacting a user. Those who experience an issue but take no action to resolve are excluded from this definition.
Observed issue	Issues that have been observed by users and no further action is taken to resolve or respond.
Complaint	A complaint occurs when a user is unable to resolve an issue themselves and require action by the platform. There are multiple avenues to report a complaint (e.g. Help Centres, real-time in app, user to user) and a process to resolve (e.g. 1:1 support; human reviews).
Internal dispute	An internal dispute occurs when a user is not satisfied with a decision made by a platform and appeals the decision. Platforms offer appeals processes to support internal disputes.
External dispute	An external dispute occurs when a user is not satisfied with a decision made by a platform and seeks to resolve by engaging with an external agency or body (e.g. ACCC, ASBFEO, state fair trading agencies).
External escalation	An alternate resolution or reporting process in response to an issue, complaint or dispute through an external agency or body, regardless of any previous attempts to resolve through the platform.
IDR	Internal dispute resolution – the process for resolving complaints and disputes with the platform
EDR	External dispute resolution – the process for resolving complaints and disputes with external body and agency (note: this can also be referred to as alternative dispute resolution (ADR)).
User-led	Users drive the resolution of issues and complaints themselves. Platforms offer a range of self-help channels with guides and prompts to encourage users to ‘self-resolve’.
Platform-led	When users cannot ‘self-resolve’ they enter the platform resolution process. This is directed by platforms and follows a series of actions taken by the platform on behalf of the user. They commonly include a review and assessment of the complaint by specialist team, and then a decision and action to resolve the complaint.
Resolution	A resolution is defined as when the user reports their issue was resolved, whether to their satisfaction or not. Unresolved issues are cases where no resolution is reached (from the user’s perspective) such as when the issue is ongoing without a resolution in sight or there were too many roadblocks for the user to progress the issue. ¹¹

¹¹ There are cases where the platform may have deemed the issue resolved and the user disagrees with this decision, which can result in dispute.

1. Diversity of the landscape

An increasingly digitised economy involves a high volume and wide range of risk and issues to resolve

Participation in the digital economy involves interactions with a range of platform types

Digital platforms are online services and applications that serve a vast array of users, and provide value based on the presence of other users or their content. Platforms can be ‘multi-sided’ with users, creators and businesses interacting in different ways to create value. For example, platforms with an advertising revenue model consist of one-side where users search or look at content, websites, goods and services, while the other side involves businesses advertising to target groups of those individuals.¹² Platforms are able to capture information on the user and their preferences which helps businesses to better target their products, and users to find what they are looking for. This has resulted in vast volumes of transactions and interactions unseen by traditional industries.

Exhibit 2 gives a non-exhaustive illustration of different types of platforms, which include:

- **Search engines:** software systems designed to enable users to search and find information online for free, generally returning a curated, ranked set of links to content websites.¹³ Search engines sell advertising for revenue purposes.
- **Social media platforms:** online services that allow users to participate in social networking, communicate with other users, and share and consume content generated by other users (including professional publishers or creators).¹⁴ Advertising is the main source of revenue for these platforms, who target ads according to user data.
- **Entertainment:** platforms that offer curated streaming content to users typically on a subscription-based service.
- **Marketplaces:** online e-commerce platforms that enable consumers to buy from a range of sellers on the platform, with the platform typically charging a fee to sellers.
- **Payments:** platforms that enable users to seamlessly pay for goods and services online with security and privacy, with fees charged to merchants or payment recipients.
- **Other:** there are a range of other types of platforms including dating, ride-sharing, health and communication applications.

While all platforms seek to bring a range of users and market actors together, the difference in function, services, transacting parties, and content gives rise to issues that differ significantly among platforms. For example, Twitter is a microblogging platform that provides a single service to its users and issues will often centre around trolling and hate speech, while Google provides search engine, video sharing, payments, email, maps and business directory services to name a few. The issues that arise from Google’s different services range from payment and consumer problems that are already regulated under Australian Consumer Law to unanticipated issues that are exacerbated in the digital age such as businesses dealing with fake reviews that they cannot remove.

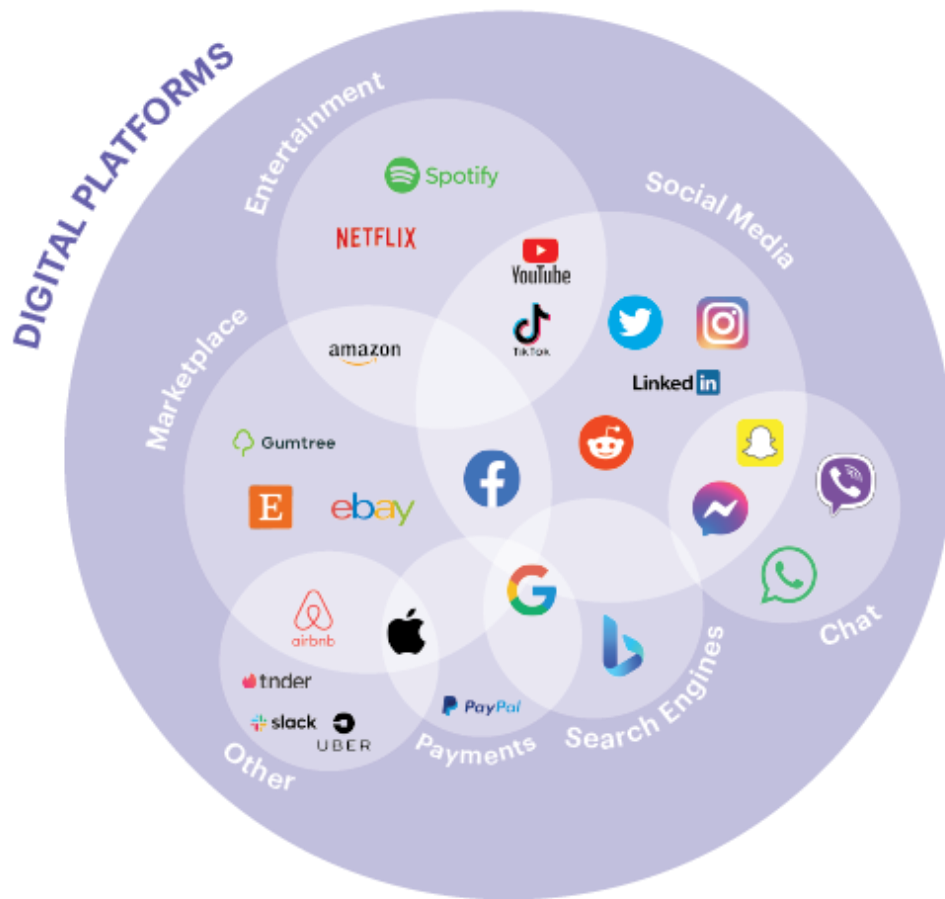
¹² ACCC [Digital Platforms Inquiry Final Report 2019](#), p 41.

¹³ ACCC [Digital Platforms Inquiry Final Report 2019](#), p 41.

¹⁴ ACCC [Digital Platforms Inquiry Final Report 2019](#), p 41.

Exhibit 2

The digital platform ecosystem involves a range of platforms*



*Indicative and non-exhaustive

Australians are increasingly reliant on platforms in our lives and businesses

In addition to the diverse range of issues that different platforms face, the adoption of digital services to address almost every aspect of consumer and business life leads to an unprecedented volume of transactions and potential issues that platforms must manage.

Exhibit 3 shows the growth in online retail sales and the percentage of Australians using different social media platforms. Around 20 million Australians are active social media users with the average internet user having 7 social media accounts.¹⁵ COVID-19 also accelerated the shift to online shopping with more than 4 in 5 Australians households making an online purchase at some point during 2020.¹⁶ As a percentage of total retail, online sales accounted for 16.3%, an amount Australia Post did not expect to reach until about 2023.¹⁷

Exhibit 3

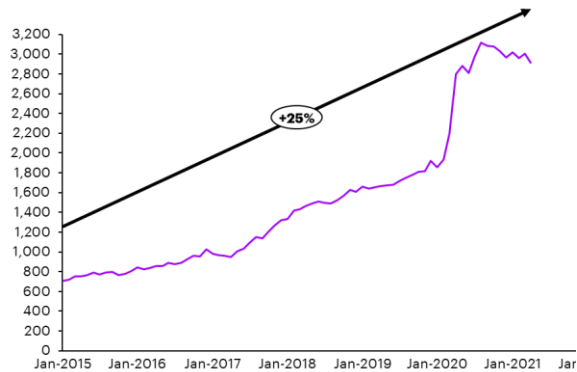
¹⁵ We are social/Hootsuite, *Digital 2021 – Australia report*, p 44, p 46; ACCC Digital Platforms Services Inquiry *September 2020 Interim Report*, p 1.

¹⁶ Australia Post, *Inside Australian Online Shopping – eCommerce Industry Report 2021*, p 4.

¹⁷ Australia Post, *Inside Australian Online Shopping – eCommerce Industry Report 2021*, p 4.

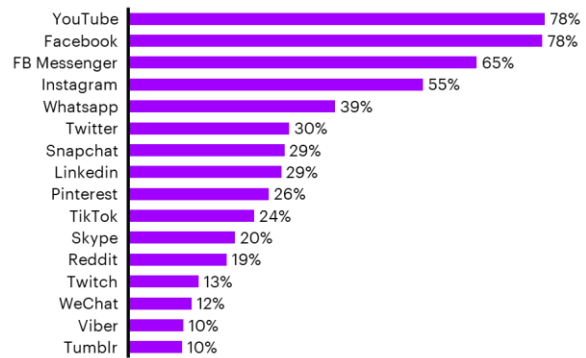
Online retail sales have grown rapidly through COVID, while social media is becoming increasingly ubiquitous

\$m monthly online retail sales Australia



Source: ABS, [Retail Trade Australia, April 2021](#) – Online sales (supplementary COVID-19 analysis)

% of internet users aged 16-64 using social media platforms (Jan 2021)



Source: We are social/Hootsuite, [Digital 2021 – Australia report](#)

With this increased penetration of digital services in our lives, platforms must respond to a high volume of user interactions, along with complex issues

The issues that platforms must address range from common customer service issues that most service providers face, to more complex issues that involve users with malevolent intentions.

Platforms' responsibilities therefore range from providing customer care to people who lose passwords or account access, reducing the presence/removing illegal content and dangerous material, bullies, internet trolls and other bad actors. Because platforms provide a public space for millions of users to transact, their issue resolution encompasses:

- standards of care that consumers have come to expect
- public functions such as ensuring safety and marketplace integrity
- scalability of these measures to the extensive array of search queries, web pages, social media accounts, messages sent, content views and other activity that occurs online
- consistency of these measures across the local jurisdictions that platforms operate in¹⁸

Exhibit 4 lists some examples of high-volume and more complex issues that different types of platforms must respond to.

¹⁸ See for example the community standards and transparency and digital trust reports of major digital platforms

Exhibit 4**There are a range of high volume and complex issues that platforms must respond to**

	Social media	Search engines	Marketplaces	Payments
# Australian users¹	20 million	22 million	9 million	3 million
High volume interactions²	<ul style="list-style-type: none"> • Lost accounts and passwords • Bullying • Content issues and policy violations 	<ul style="list-style-type: none"> • Managing business and publisher accounts • Managing listings and business statuses 	<ul style="list-style-type: none"> • Customer satisfaction with delivery of goods and services • Payments 	<ul style="list-style-type: none"> • Logins and status of payments
	<ul style="list-style-type: none"> • Advertising related applicable to all: buying and selling ads, managing ad accounts, responding to ad listing changes 			
Complex issues²	<ul style="list-style-type: none"> • Fake accounts can be difficult to ascertain • Scams are prevalent and require constant monitoring • Users are at risk of accounts being hacked by global bad actors 	<ul style="list-style-type: none"> • Fake reviews are difficult to assess and need to balance freedom of opinion • Business understanding of page rank algorithms and advertising products • Managing the potential for illicit or prohibited content on search results 	<ul style="list-style-type: none"> • Disputes between buyers and sellers require judgements by the platforms • Sellers may engage in misleading or deceptive conduct, or anomalous pricing behaviour 	<ul style="list-style-type: none"> • Hacking of accounts • Disagreements between buyers and sellers
	<ul style="list-style-type: none"> • Advertising related applicable to all: ad visibility, efficacy, engagement and transparency 			

Sources: (1) Data for social media and search engine users in Australia are from [We are social/Hootsuite Digital 2021](#) - Australia report, users on online marketplaces are from [Neto State of Ecommerce Report 2018](#), and users on payment platforms are from RBA Bulletin "[Developments in the Buy Now, Pay Later Market](#)" March 2021. (2) Stakeholder engagement with platforms, industry bodies and regulatory agencies

This study focuses on a subset of these issues

Of the myriad issues that users face on digital platforms, this study focuses specifically on the issues listed in **Exhibit 5**. A taxonomy of issues was developed in conjunction with the Department based on the key risks and issues identified in the Digital Platforms Inquiry. Several complaint and issues categories were excluded as outlined further below, that are already being addressed by existing laws and regulation.

Exhibit 5**A defined set of issue types were considered in this report**

Categories of issues	Description
Payments	<i>Payment and transaction issues between users on a platform that has a payment system or functions as a marketplace.</i>
Spam	<i>Content that is unsolicited, annoying and usually posted or sent in bulk to users.</i>
Scams	<i>Content that is false and designed to trick users into spending money, sharing their personal information etc. Includes online shopping, investment, dating scams, fake ads and phishing.</i>
Fake reviews	<i>Fake reviews or comments e.g. fake reviews on a business page to boost sales, or fake, vexatious complaints received from unsatisfied customers.</i>
Hacking and fake accounts	<i>Account hacking or fake accounts created to mimic another user, or fake accounts created to engage in offensive or inauthentic behaviour.</i>
Content or account removal	<i>When a platform suspends or removes an account or removes content posted by a user. For businesses this can result in loss of followers or customer data on the platform.</i>
Ad-related issues	<i>Issues around ads such as being incorrectly billed for an ad, ad not delivering promised or expected results, transparency around ad effectiveness and unexpected changes to platform algorithms that reduce ad visibility.</i>
Platform policies and procedures	<i>Issues that users have with the platform's complaint handling policies and processes. Examples include where users cannot find information on how to make a complaint or contact the platform, and where users are told they are in breach of platform guidelines but do not know which provision.</i>

While users experience other issues that platforms must respond to (see **Exhibit 6**) these are not the focus of the study as prohibited content is covered by existing laws and regulation (e.g. eSafety Commissioner, Office of the Australian Information Commissioner). Relatively minor issues such as lost passwords and logins are also not considered. Although certain issues are outside of scope, interactions can still exist between categories included and those excluded e.g. a fake account being used to bully someone. These issues are complex and sometimes multifaceted – a clear delineation is almost impossible. In presenting the data, the default is to how the user would best describe and categorise their issue.

Exhibit 6**Several issue types are out of scope**

Categories of issues	Description
Offensive content	<i>Content that offends other users such as bullying and harassment, adult nudity and sexual activity, violent and graphic content.</i>
Prohibited or regulated content	<i>Content that is legally restricted e.g. child nudity, terrorism.</i>
Public misinformation	<i>Information intentionally or unintentionally deceptive or misleading that affects the public interest.</i>
Infringements (IP, privacy)	<i>Content that violates someone's privacy (e.g. someone's address, IDs, health records) or copyright or trade mark laws.</i>
User error	<i>Can include issues such as lost passwords and logins</i>

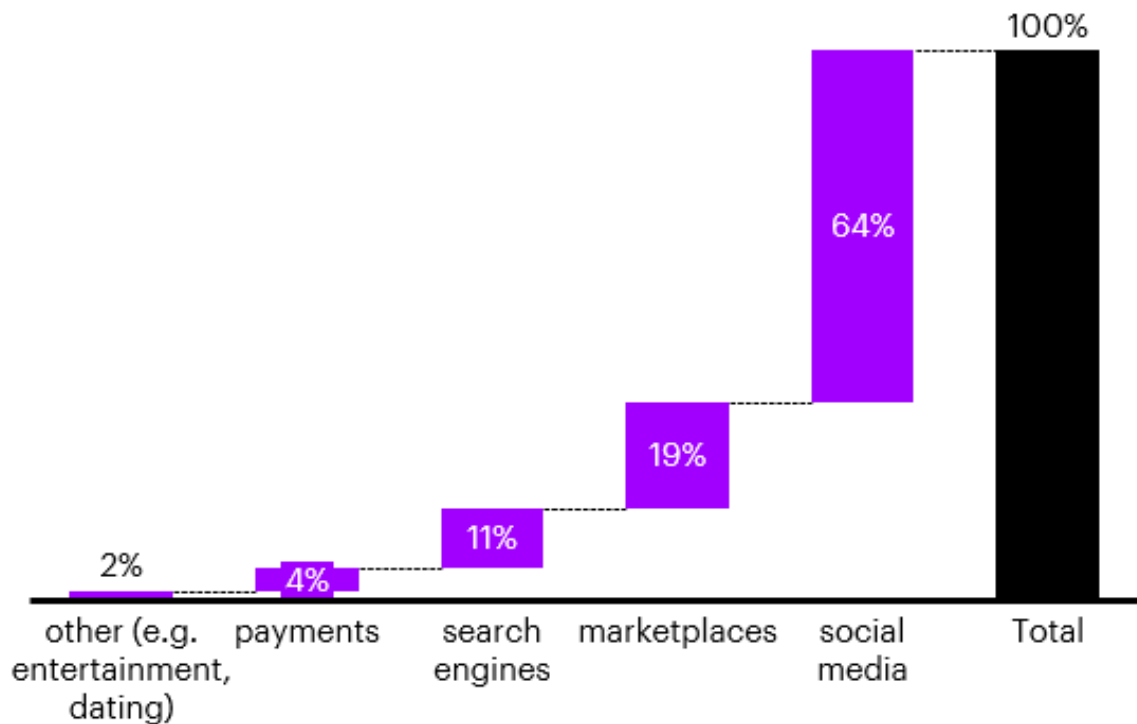
The survey results indicate that the issues which occur on platforms vary significantly by platform type (see **Exhibit 8**). The diversity of issues and prevalence of issues, complaints and disputes is dependent on the service offering and platform type. Social media platforms respond to the highest share of issues—due to the high penetration of users—and have a higher proportion of hacking and fake accounts, while search engines have a lower share and respond to more scams and fake review issues (see **Exhibit 7**). As expected, marketplaces have the highest share of payment and scam issues.

Exhibit 7

Social media platforms have the highest share of issues

User issues by platform type

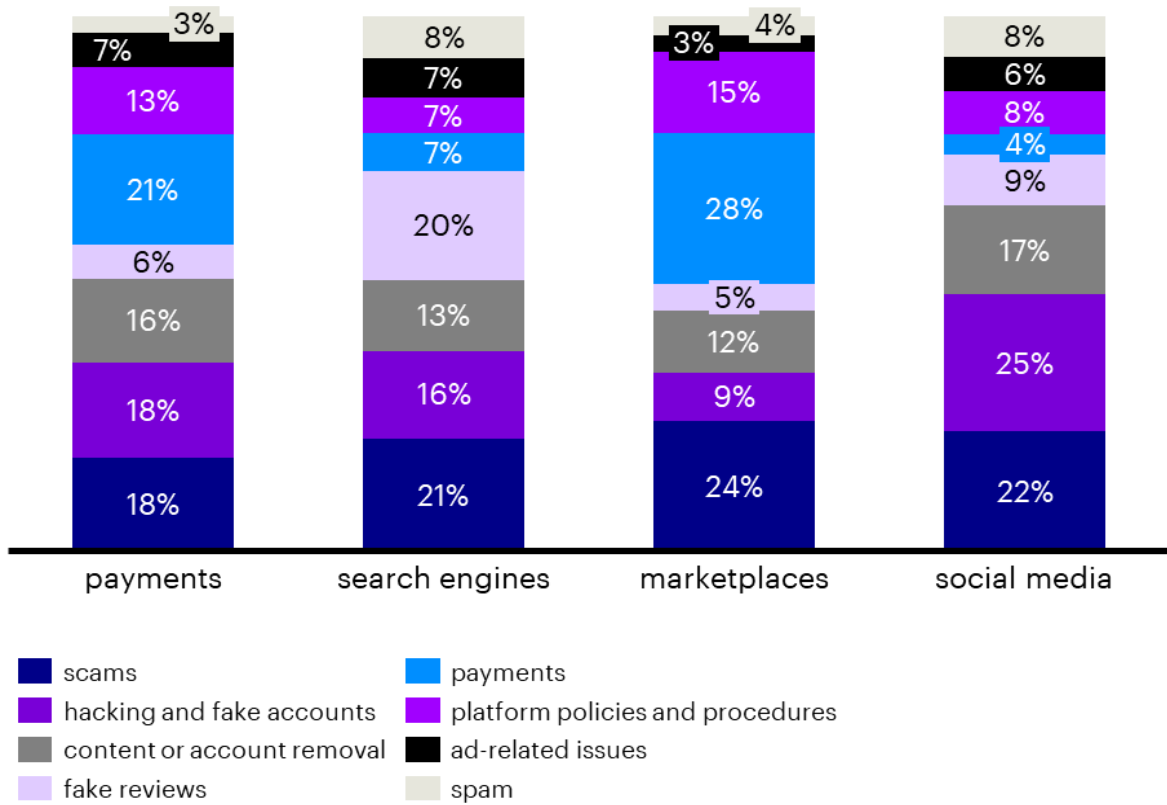
% of user issues, complaints and disputes



Source: Analysis of consumers and businesses who have experienced an issue, complaint or dispute that is within the scope of this study

Exhibit 8**The composition of issues differs by platform type**

Composition of user issues by platform type
 % of user issues, complaints and disputes



Source: Analysis of consumers and businesses who have experienced an issue, complaint or dispute that is within the scope of this study

2. Context of issues

Many of these issues are not new

A number of these issues existed prior to the emergence of digital platforms, albeit at a lesser scale:

- **Scams:** scams have historically occurred through more traditional communication forms, with 50% of scams today still delivered through telephone.¹⁹
- **Payments:** payment issues occur through financial institutions, which have now translated to financial intermediaries and payment applications supporting online transactions.
- **Spam:** spam has historically been an issue through mail but can now occur on a much larger scale and frequency through social media and email.
- **Platform policies and procedures:** most goods and services have terms and conditions which can be disputed or cause dissatisfaction with users. Complaints around inability to contact a customer service representative, or how the policies surrounding a good or service are applied to customers, are also not unique to digital platforms.
- **Ad-related:** issues around the effectiveness of advertising have existed on traditional media forms such as television, newspapers and other publications. The availability of data to track ad performance on digital platforms creates new issues as ad-buyers expect more transparency and solutions to problems that were not traditionally able to be tracked or identified. For example, there have been cases where platforms have misled advertisers with inaccurate information and data about their advertising products.²⁰
- **Content or account removal:** consumers and businesses could traditionally have their account removed or access revoked to a whole range of goods and services. However, digital platforms are playing an increasingly critical role where account or content removal can have a much larger impact.
- **Hacking and fake accounts:** while individuals could historically impersonate other businesses or users, the impact of engaging in this conduct online is much higher given the ability to hide your identity and reach large audiences.
- **Fake reviews:** although fake reviews could potentially occur through traditional media forms, the reach and visibility of reviews on digital platforms means that the impact of fake reviews can be much higher.

While these issues existed in the past, the accessibility (anyone with internet on their phone or computer), availability (free or low cost), expanded reach (from local, to national to global) of digital platforms has exacerbated the scale of these issues.

¹⁹ ACCC [Scamwatch](#)

²⁰ Sydney Morning Herald 2020, '[Facebook apologises for misleading advertisers](#)'

Some regulatory arrangements are in place to support resolution of these issues, but shortcomings do exist

The wide range and scale of issues requires a diverse set of capabilities to be able to support the resolution of these issues. There are a range of ombudsmen and federal and state agencies in place to support potential appeals and disputes on digital platforms for each complaint type as shown by **Exhibit 9**. However, issues on internationally-based digital platforms present new and complex challenges for existing regulators and ombudsmen. Most complaints will involve a potential breach of contract (platform terms and conditions) or a breach of the Australian Consumer Law, though some may also involve a crime.

There are some limitations on jurisdiction of these external parties to support dispute resolution on digital platforms. Disputes around a platform's terms of service may not be a breach of Australian Consumer Law (ACL), and agencies do have limited enforcement powers in these circumstances. In addition, some of the digital platforms' terms of service require litigation to be held in foreign courts where the platforms' headquarters are located. This can make the judicial process very costly and complex.²¹ However, it should be noted that platforms often do coordinate with external agencies to resolve disputes even when there is an absence of power to enforce a resolution. The responsibilities and limitations of each of the relevant external agencies and legislation is summarised in the appendix in **Exhibit 37**.

Exhibit 9

There are existing regulatory arrangements in place for issues on digital platforms

Categories of issues	Description	Relevant legislation
Scams	Scams can be reported to ACCC's Scamwatch, or complaints made to state fair trading and consumer affairs bodies. Scamwatch will gather data and identify trends or systemic issues but it does not help individuals resolve issues. Success of these channels will depend on the ability to track the offending party down.	Australian Consumer Law, criminal law for certain scams
Payments	Australian Financial Complaints Authority (AFCA) can consider complaints about a banking deposit or payment issue, including internet banking and mistaken internet payments. ²²	Australian Consumer Law; Australian Securities and Investments Commission Legislation and other associated regulation.
Spam	Spam can be reported to ACMA. ACMA can investigate serious spam complaints, but this is limited to spammers based in Australia who can be tracked down rather than the carriage service providers.	Australian Consumer Law, Spam Act, Telecommunications Act

²¹ See for example [Australian Information Commissioner v Facebook Inc](#) (No 2) [2020] FCA 1307; Dow Jones v Gutnick (2002) 210 CLR 575

²² If a platform does not have a Financial Services Licence, any dispute that arises within the context of the operation of a platform or marketplace must be raised against the licensed entity, with any action on the part of the platform largely the result of goodwill on their part or trying to minimise reputational harm.

Platform policies and procedures	<p>Depending on the nature of the complaint, consumers can complain to the OAIC, ACCC, or state fair trading and consumer affairs bodies, while businesses can complain to the ASBFEO or state-based small business commissions.</p> <p>Many of these complaints do not involve a breach of contract or a breach of the ACL. As a result, it is often not clear how disputes arising from an unfair application or interpretation of the platform's policies and procedures can be resolved.</p>	Privacy Act, Australian Consumer Law
Ad-related issues	Complaints about advertising products may relate to a breach of Australian Consumer Law, and can be directed to the ASBFEO, ACCC or state-based fair trading and consumer affairs bodies or small business commissions. ²³	Australian Consumer Law
Content or account removal	<p>Possible avenues will depend on the specific context surrounding the removal. If the content or account removal was related to an issue of cybercrime or bullying, then the user can make a complaint to the eSafety Commissioner. If it was related to a consumer or small business issue, then the user can complain to state fair trading and consumer affairs bodies.</p> <p>It can be difficult to appeal account or content removal processes as it is typically a violation of the platforms' terms of service rather than ACL.</p>	Enhancing Online Safety Act, Australian Consumer Law
Hacking and fake accounts	Victims of a cybercrime, such as hacking, online scams or fraud and identity theft can report to the Australian Cyber Security Centre.	Criminal law, Australian Consumer Law, Enhancing Online Safety Act
Fake reviews	Fake reviews can be reported to the ACCC, ASBFEO or state-based fair trading and consumer affairs bodies or small business commissions.	Australian Consumer Law

²³ Actions for misleading or deceptive conduct are only likely to be successfully brought against an entity with either a presence or assets within Australia.

3. Advantages and challenges

Addressing these issues in a digital context has both advantages and challenges

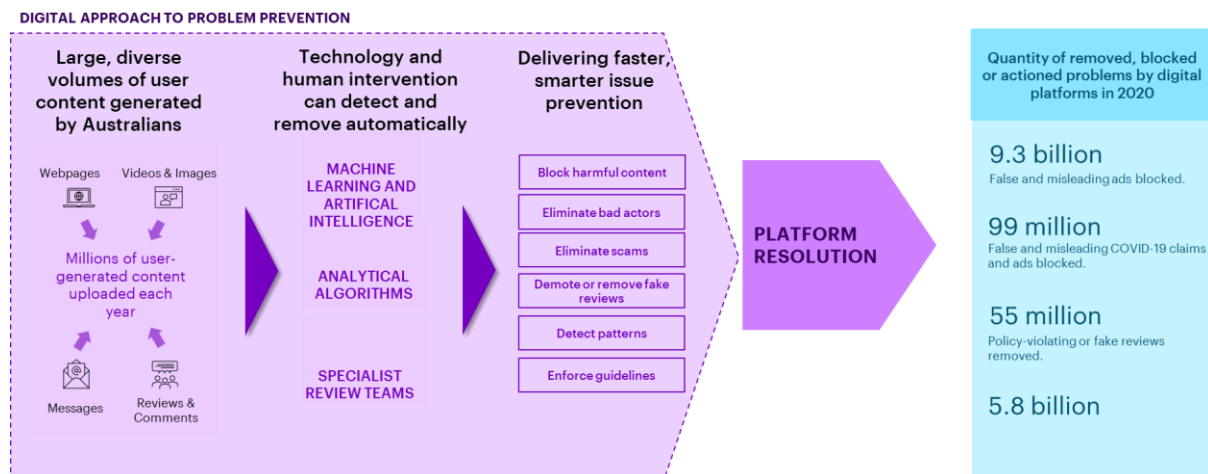
Platforms can prevent most of these issues before they happen using technology

There are a number of benefits to addressing these issues in a digital context. Platforms use issue prevention processes and technologies to dramatically reduce users' exposure to harmful and malicious materials. Machine learning, AI and specialist review teams work proactively to block harmful content, eliminate bad actors and scams, demote or remove fake reviews and enforce guidelines.

Exhibit 10 illustrates some of the ways platforms detect and remove issues automatically. Globally, platforms take action on billions of problematic content or behaviour each year, and most of it proactively. For example, in 2020 9.3 billion false and misleading ads and spam were blocked, 55 million policy-violating or fake reviews were removed, and 5.8 billion social media accounts actioned including fake accounts.²⁴ The majority of these are captured by AI and other technology. s47G - business information

Exhibit 10

At a global scale, platforms prevent billions of potential problems from occurring



Source: (1) Global figures, provided by digital platforms and transparency reports

Notes: global statistics of removed, blocked and actioned content by digital platforms is mostly done proactively by platforms before users experience them

For those issues that do make it through, platforms have put in place several measures to support prevention and rapid issue resolution. Users are encouraged to initially self-resolve issues for timely and convenient resolution, in addition to several measures that platforms undertake to prevent and resolve issues (see **Exhibit 11**). For example, Google uses both people and technology that closely monitor Maps 24/7 who can take swift action against scammers, ranging from content removal and account suspension to litigation. In 2020 Google took down more than 960,000 reviews globally, and more than 300,000 Business Profiles that were reported by Google Maps users.

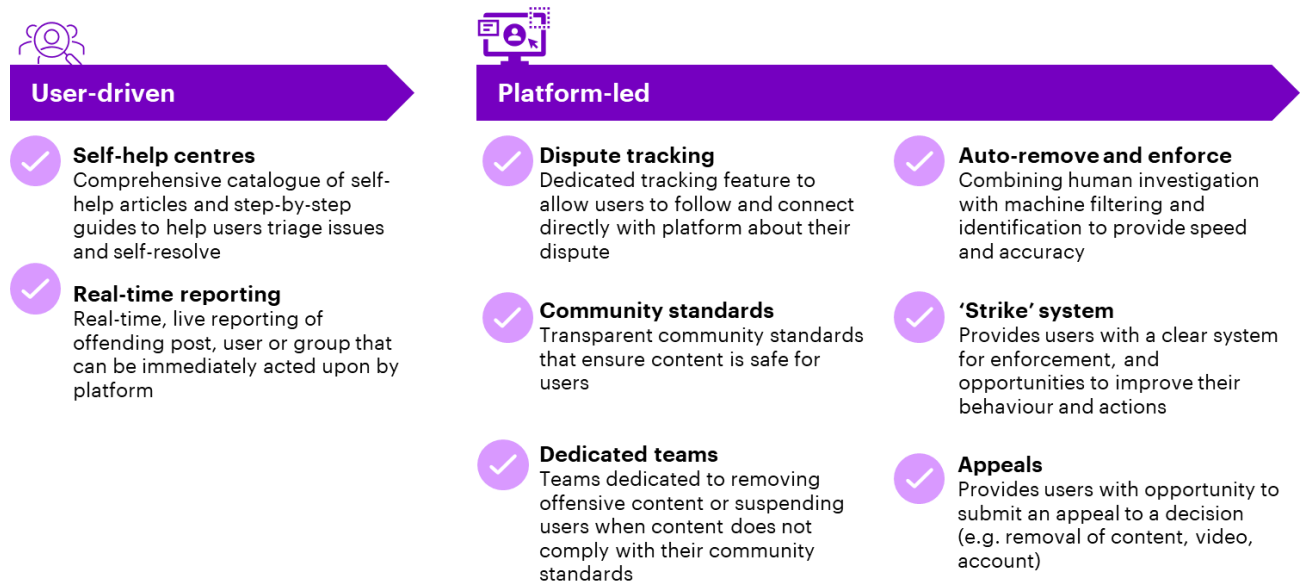
²⁴ Global figures, provided by digital platforms and transparency reports

"I was preparing for this to take a week. All happened straightaway...as it should I guess" – User interview

"They came back straight away and were clear about what would happen next – I knew they were on it" – User interview

Exhibit 11

Platform capabilities support prevention and rapid issue resolution



Source: desktop research, interviews with government agencies, information from platforms, analysis and synthesis of consumer interviews

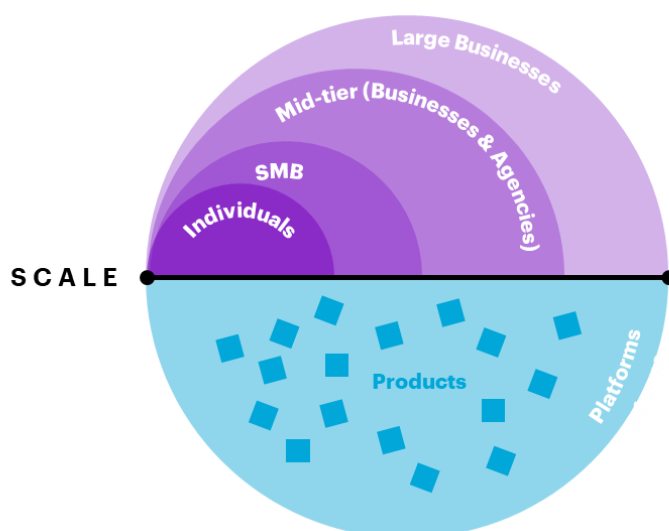
However, there are challenges in a digital environment

While the digital environment has enabled AI and algorithmic methods to filter out a large number of issues, it has also created new challenges specific to the scale that digital platforms operate in. Platforms must respond to the different needs and expectations across user segments and across each of their product areas, while users must contend with processes and procedures that are designed to operate efficiently at a global scale, but are less tailored to the individual or their location.

Platforms may have product lines that operate independently of each other (e.g. Google's YouTube and Google Maps) which respond differently depending on to the product and type of issue. Platforms that operate more than one product have indicated that it is difficult or may not be suitable for them to adopt the same issue resolution procedure across all products.

Exhibit 12

Managing issues on digital platforms can be complex given the range users, product



Source: desktop research, information from platforms

In addition, platforms face unique challenges in providing a virtual public place for people to meet and transact. In doing so, they must:

- **Ensure the integrity** and safety of platforms and marketplaces
- **Protect others** and the public from bad actors
- **Enforce community standards** and minimising the risk of prohibitive or illicit content
- **Manage vast volumes of global interactions** and the subjective nature of potential issues.
Managing billions of user interactions across borders involves dealing with the unique language, culture, regulations, and legislation of each country.

There are also difficulties in resolving disputes in a digital context. External agencies may not have jurisdiction to mediate, arbitrate or enforce a decision for a platform. In addition, based on the platforms terms and conditions, disputes and appeals may require users to litigate platforms in foreign courts.

Platforms have limited control over how users behave on the platform in some contexts, but at the same time must have efficient and scalable measures in place to police and act on bad behaviour—sometimes in very subjective contexts—over billions of users. For some users this might result in content or account removal that is not explained, appears heavy-handed, or is incorrect if the platform had a better understanding of the cultural context. This in turn creates more user issues and complaints.

4. Mapping dispute resolution

Digital platforms have developed a range of scalable and innovative approaches that prevent most issues from becoming a dispute

When a consumer or business experiences an issue, complaint or dispute, there are four core stages of resolution:





- Platform resolution
 - user driven approaches such as resolution with other users, self-help guides community forums; or
 - platform-led processes through webforms or in-situ report.
- External disputes or escalation
- Judicial resolution

Exhibit 13 describes each of these stages, their key functions, stakeholders, and the overall ability to resolve.

Platform resolution that is user-driven enables resolution in real time, with users self-resolving by using online tools such as prompts and FAQs, or they can engage in user-to-user resolution by communicating directly with another user, group or community to try and resolve the issue. Platform-led processes enable the user to report an issue directly to the platform, normally by filling in a questionnaire, which is then assessed and actioned by the platform. For example, with regard to scams and misleading content, anybody can report an ad for review on Google by filling out a simple “Report an Ad” web form. If the user disagrees with the outcome determined by the platform, they can appeal by raising an internal dispute with the platform. **Exhibit 14** illustrates the platform resolution processes.

Exhibit 13

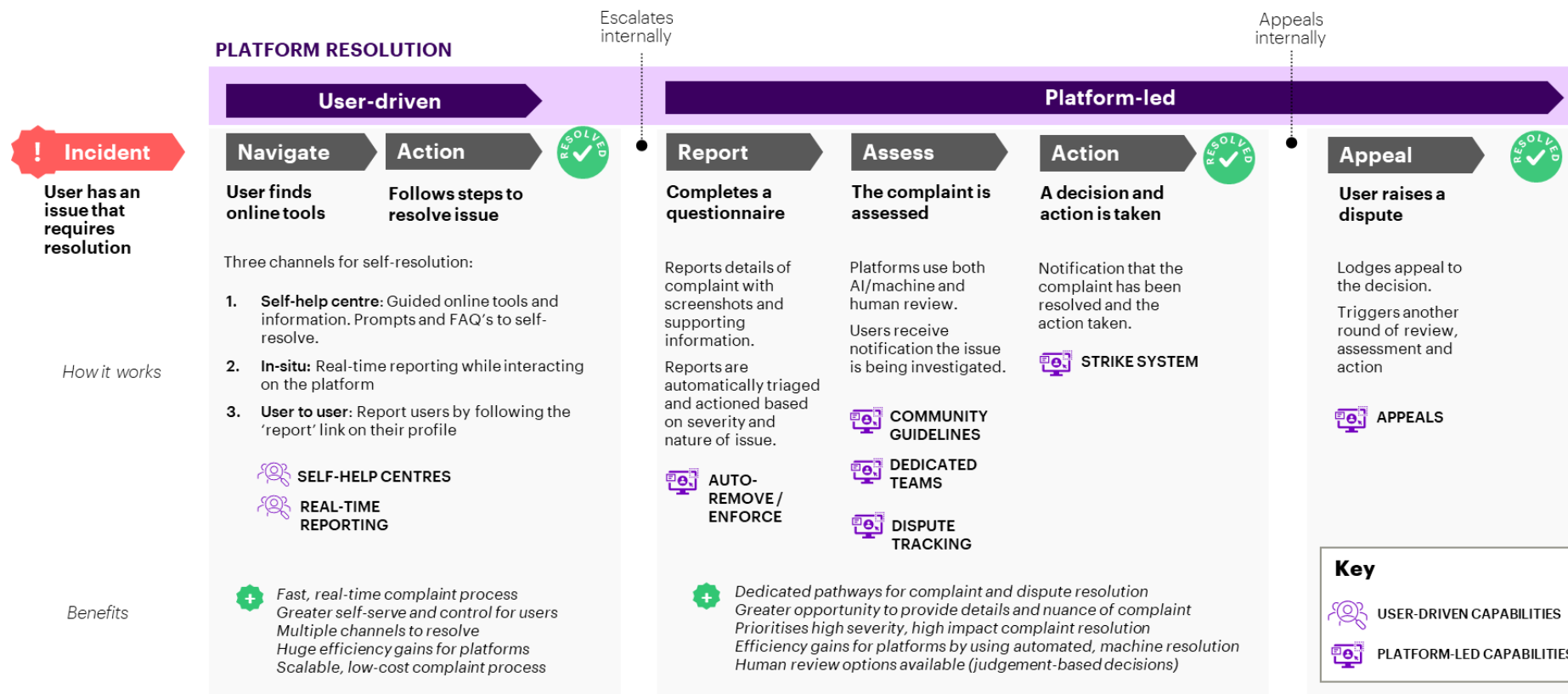
There are four core stages of issue, complaint and dispute resolution

	PLATFORM RESOLUTION User-driven Platform-led		EXTERNAL ESCALATION	JUDICIAL RESOLUTION
DESCRIPTION	Users engage the platform directly and are guided to self-resolve their complaint. They follow steps outlined in platform FAQ's or message boards/communities. Complaints can also be resolved directly between users when appropriate.	If users cannot resolve complaints themselves, they are typically guided to contact the platform through a webform or other in-situ method.	When a user cannot contact the platform or requires advice and guidance to resolve their complaint, they engage an external party. Users can also report content to external agencies (e.g. Scamwatch).	Finally, when other channels are exhausted users can resort to litigation, which often involves a lengthy process and costly legal fees
KEY FUNCTION	Provides tools and information to enable users to 'self-resolve' their complaint/dispute	Assesses a complaint/dispute and acts on behalf of the user	Triage complaints, educates users on their rights and provides guidance on next-steps	Enables dialogue between the user and the platform, mediating and enforcing a resolution
KEY STAKEHOLDERS	<ul style="list-style-type: none"> • User (consumer or business) • Other users • Communities and forums 	<ul style="list-style-type: none"> • Digital platforms • User (consumer or business) 	<ul style="list-style-type: none"> • Digital platforms • State and Federal police • ACMA • ACCC • ASBFEO • Fair trading agencies • Ministers • DITRDC • Consumer groups • TIO 	<ul style="list-style-type: none"> • State and Territory Civil and Administrative Appeals Tribunal • Local Courts • District (or County in Vic) Courts • State or Territory Supreme Courts • Federal Courts • High Court of Australia
ABILITY TO RESOLVE	 Self-resolution can be achieved directly between a user and other users, groups or communities	 Resolution can be achieved on behalf of a user with a range of enforcement options	 Agencies can enforce in some circumstances but there are limitations on a case-by-case basis, and often require direction back to the platform	 Resolution can be achieved, however there are significant barriers such as the potential requirement to litigate overseas, as well as time and financial costs.

Source: desktop research, interviews with government agencies, information from platforms, analysis and synthesis of consumer interviews

Exhibit 14

Platform resolution delivers an efficient journey for most complaints



Source: desktop research, information from platforms

Platforms apply a range of innovative capabilities depending on their service offering

While most platforms have a baseline level of resolution processes (see **Exhibit 11**) to support users in resolving issues, some companies have come up with additional unique capabilities tailored to their different offerings and functions. s47G - business information



s47G - business information

FACEBOOK

s47G - business information

s47G - business information



s47G - business information



s47G - business information

Even though platforms have resolution capabilities in place, 4.2 million issues are still experienced by users

Survey data suggests that each year, around 4.2 million issues are still experienced by users. Of these issues that are experienced, some will result in a complaint, others in an internal dispute or external dispute, and some may be left unresolved. 16% of issues remained unresolved, which can occur at any stage in the funnel when the user has received no resolution. For example, the matter is ongoing with no resolution in sight, or the user has chosen to withdraw an issue because of roadblocks (e.g. not being able to speak to the right person). Resolved issues, complaints and disputes can be perceived as satisfactory or

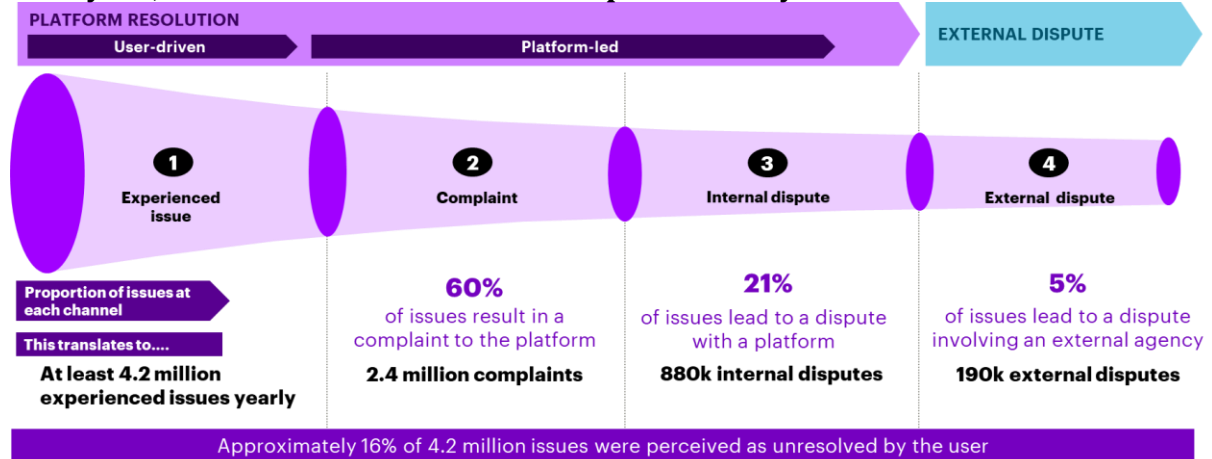
²⁷ Facebook 2019, '[An Update on Building a Global Oversight Board](#)'

unsatisfactory by the user. For example, a user may be unsatisfied if they dispute content removal but the platform ultimately decides that the content was in violation of their community standards and does not reinstate it.

Exhibit 15 is a funnel which shows of the 4.2 million issues, how many result in a complaint, internal dispute, external dispute or are left unresolved. It is important to note how each of these categories are defined:

- **Issues:** in the survey, an **experienced issue** is defined as a problem a user experiences on a digital platform. This could include, for example, resolving a payment issue on a platform between a buyer and seller without involving the platform. Issues exclude the **prevented problems** that platforms manage (e.g. through AI) before any user has even been impacted. Each year there is an estimated 4.2 million issues experienced on platforms each year. 1.6 million of these are resolved while the remainder were escalated as a complaint to the platform, and a small proportion (149,000) escalated or reported to external agencies without contact with the platform.
- **Complaint:** an issue becomes a complaint to a platform when the user contacts the platform directly to resolve the issue, such as complaining about the removal of their content on a platform. The most common way of making contact was clicking a reporting link on the platform. Of the 4.2 million issues, 2.4 million resulted in a complaint to the platform. 1.1 million of these were resolved, 353,000 were unresolved, 115,000 escalated or reported to external agencies and the remainder resulting in internal dispute.
- **Internal dispute:** occurs when the platform makes a decision regarding a complaint that the user disagrees with *and follows up with the platform*. Examples of this can include appealing a decision or action a platform took against a user, such as a removal of an account after an initial complaint to restore the account. 21% of the experienced issues resulted in an internal dispute (880,000), with 518,000 of these being resolved, 173,000 unresolved and the remainder resulting in an external dispute.
- **External dispute:** occurs when the user contacts an external body to try and resolve, after attempting to resolve the dispute through the platform.²⁸ An example of this could be a fake review that a business requests to be removed within the platform. If the business cannot get a resolution within the platform, they may dispute this through an external body like the ASBFEO. 5% of experienced issues result in external dispute (190,000), of which 130,500 are resolved.

²⁸ This figure excludes those which are reported to a third party but do not involve a dispute with the platform (264,000).

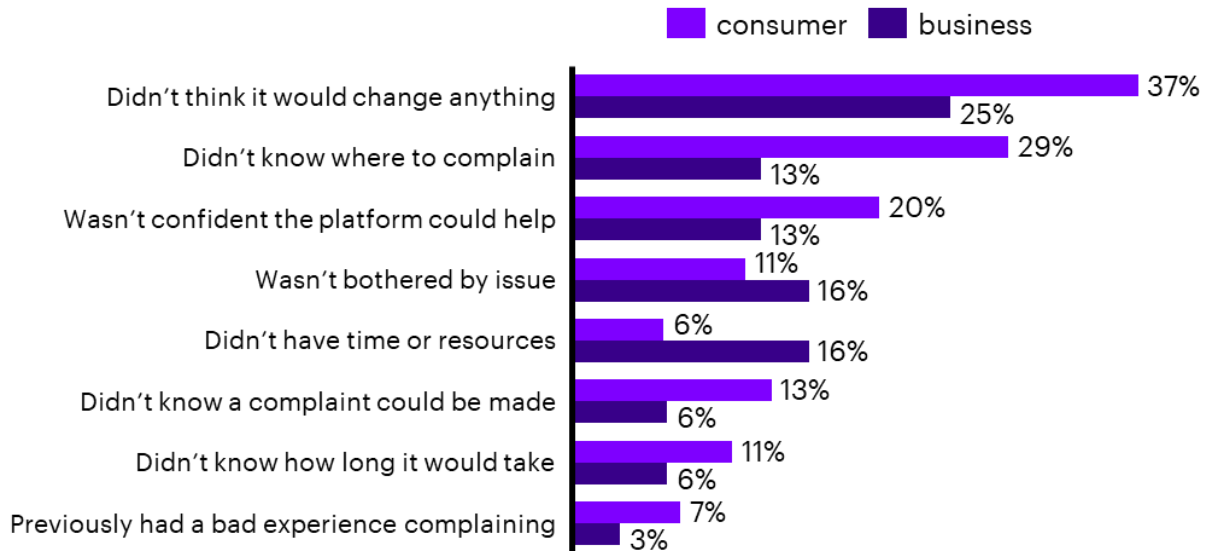
Exhibit 15**Each year, there are 4.2 million issues experienced by users**

Source: Analysis of consumer and business survey

In addition to the 4.2 million issues that were experienced by users, there were 622,000 consumer and 115,000 business issues that were observed, where no action was taken. Users did not take action for several reasons including concluding it would not change anything, not knowing where to complain, lacking time or were not bothered by the issue (see the exhibit below).

Exhibit 16**Each year there are 622,000 consumer and 115,000 business issues observed where the user chooses not to take any action to resolve**

% of consumers and business who observed an issue but did not take action



Source: Analysis of consumer and business survey

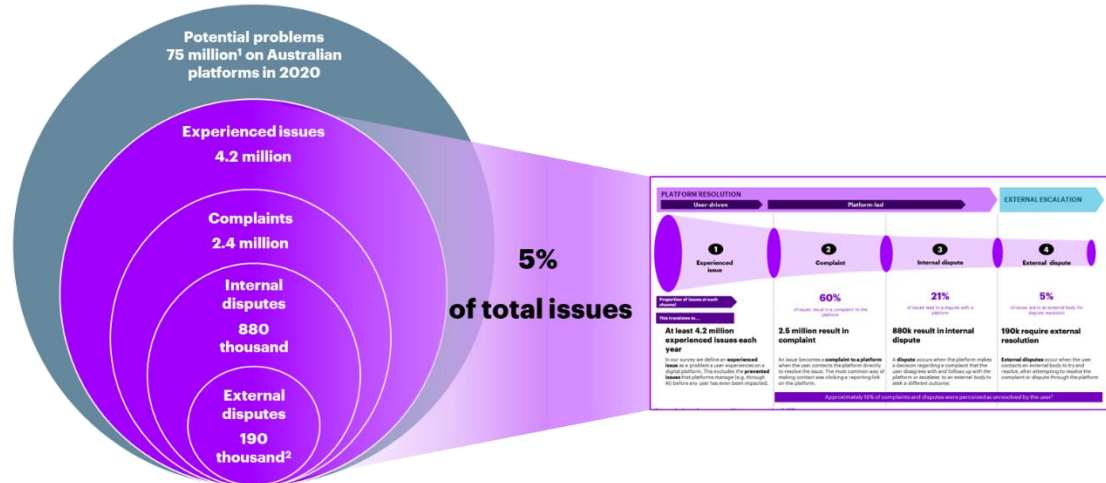
However, 4.2 million experienced issues is only 5% of the total number of potential problems platform capabilities prevent

As seen in **Exhibit 17**, data provided by digital platforms and global transparency reports claim that there are approximately 75 million potential problems that occur on digital platforms each year. 95% of these potential problems are prevented proactively by platforms using machine learning, artificial intelligence,

analytical algorithms and specialist review teams to detect and automatically remove issues before users experience them. The 5% that remain make up the 4.2 million issues experienced by users.

Exhibit 17

Platforms prevent 95% of potential problems from being experienced by users



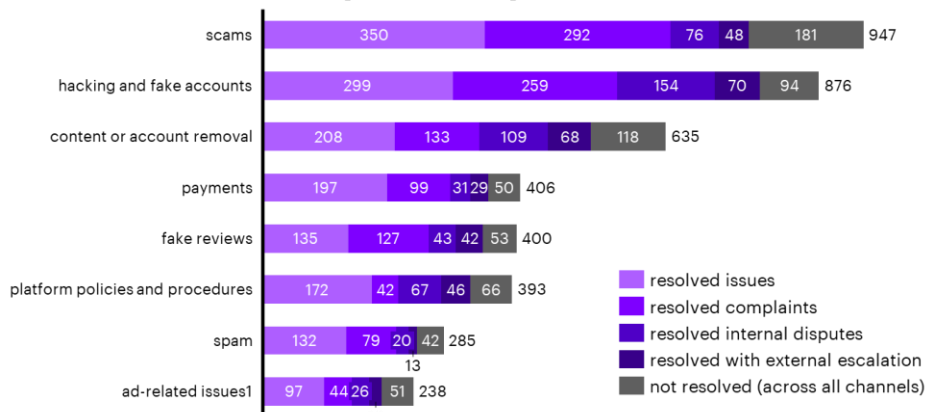
Source: Analysis of consumer and business survey; (1) data provided by digital platforms; global transparency reports Notes: (2) Excludes those which are reported to a third party but do not involve a dispute with the platform (264K).

Exhibit 18 shows that most issues and complaints are resolved within the platform before they become a dispute or are escalated externally.

Exhibit 18

Most issues and complaints are resolved within the platform before they become a dispute or are escalated externally

Thousands of user issues, complaints and disputes



*Ad-related issues only apply to businesses. Source: Analysis of consumer and business survey

Scams make up the highest volume of complaints but are also most likely to be resolved before the issue escalates to a complaint or dispute. A majority of these scams are minor such as seeing a fake ad or an online shopping scam. Around 1 in 6 said they were the target of a romance or investment scam.

Hacking and fake accounts have the second highest volume of complaints due to most of these issues occurring on social media platforms, which have the highest number of users. These types of complaints also have the lowest likelihood of being unresolved or leading to an external dispute which indicates that these types of complaints are being dealt with more effectively relative to other complaints.

Content and account removal issues often stem from other issues that platforms have had to address. For example, a platform may have removed content that it deemed offensive, however, the user disagrees and raises a complaint with the platform. In addressing an issue, platforms can sometimes create another. This highlights the complexity of the types of complaints platforms have to manage.

Almost half of payment issues, complaints and disputes are resolved as an issue with the user self-resolving or resolving with another user, group or community. This is likely due to both consumers and businesses stating that the information/help centre was easy to find (highest out of any other platform type). Additionally, over 90% of both consumers and businesses said that the instructions on payment platforms on how to resolve issues were very clear.

Fake reviews are lower in overall volume as they are typically only faced by businesses but are challenging for platforms to investigate as there are instances of businesses claiming a fake review when it is not a fake review, just a bad review. The platform has to investigate the matter from both sides (the business and the reviewer) to make a decision and this can draw out the process. In cases where a business has been falsely reviewed, the length of time it takes platforms to investigate and remove the review can have significant impacts on a business's reputation and profitability.

"The process took a week. I had to prove who I was, prove they weren't legitimate, before they (platform) investigated." - Business interview referencing a fake review complaint

Issues with a platform's policies or guidelines are low in volume but have a higher chance of leading to a dispute. These issues are difficult for platforms to solve using scalable approaches or for users to self-resolve. Ad-related issues result in the highest proportion of unresolved issues, however there is a lot of variation within this category. Uncontroversial issues like being wrongly charged for an ad are almost always resolved. More subjective issues like an ad not delivering the expected results have much lower rates of resolution.

Platform resolution is faster and results in higher satisfaction, however more complex complaints may be more likely to be escalated to external bodies

In the survey, respondents were asked to state how long it took to resolve their issue, complaint or dispute, and to indicate whether or not they were satisfied with the resolution given (when asked the status of the issue, complaint or dispute, respondents were given the option to answer 'ongoing', 'withdrawn', 'resolved – satisfied', 'resolved – unsatisfied').

Exhibit 19 shows the average number of days it took to resolve the issue, complaint or dispute and the percentage of users who responded 'resolved – satisfied' by channel.

Descriptions of channels:

- **External agency:** User pursues an external agency (e.g. ACCC, ASBFEO) to help resolve their issue.
- **Complain to platform:** User complains directly to the platform to resolve an issue. According to survey data, many consumers (44%) contacted the platform by clicking on a reporting link on the platform.
- **User to user resolution:** User resolves complaint with another user. For example, a business that receives a problematic review on their business page might reach out to the reviewer privately to resolve an issue.

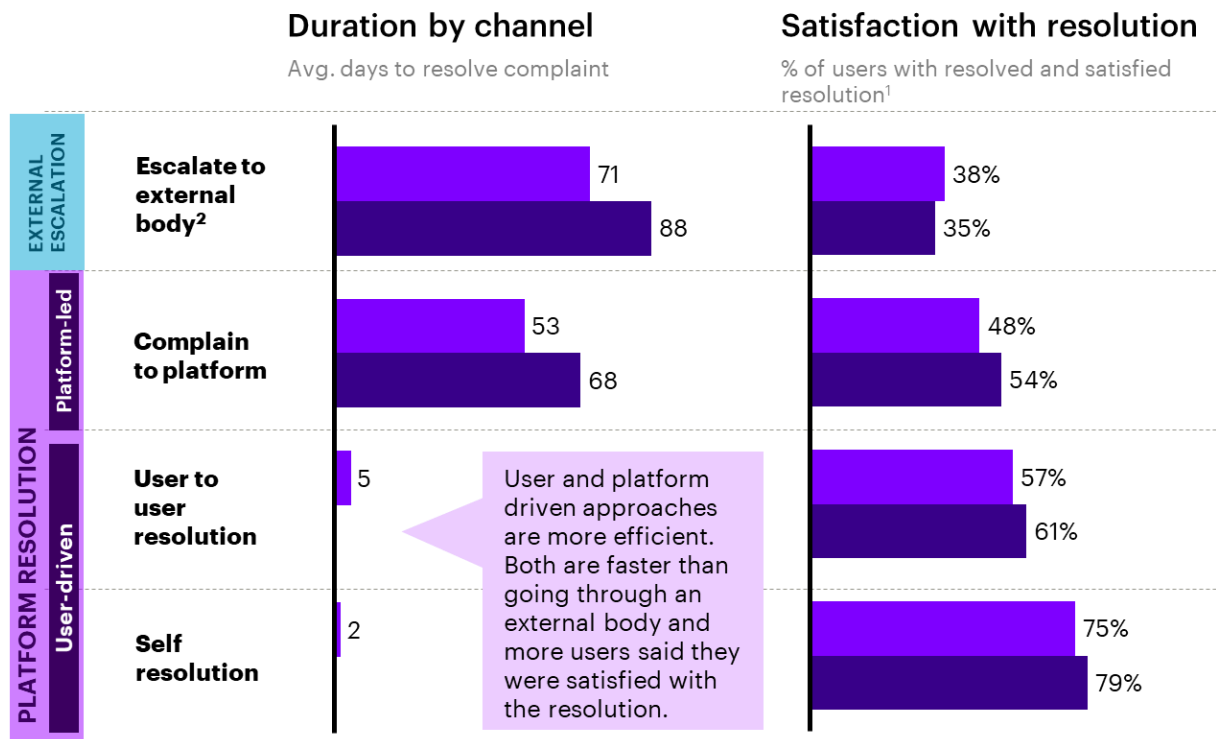
- **Self-resolution:** User utilises the platform's self-help features such as FAQ guides or community forums to resolve their issue.

Consumers and businesses indicate highest satisfaction with resolution from platform resolution processes. User-driven processes which tend to be actioned and resolved immediately have the shortest duration, on average between 2-5 days. External escalation has the longest duration, lasting on average 71 days for consumers and 88 days for businesses.

Exhibit 19

Platform resolution is faster and results in higher satisfaction

■ consumers ■ business



Source: Analysis of consumer and business survey

Notes: (1) the remainder include ongoing, withdrawn, and resolved unsatisfied (2) Includes both external disputes and issues escalated to external bodies

User driven and platform driven approaches cost less than external resolution

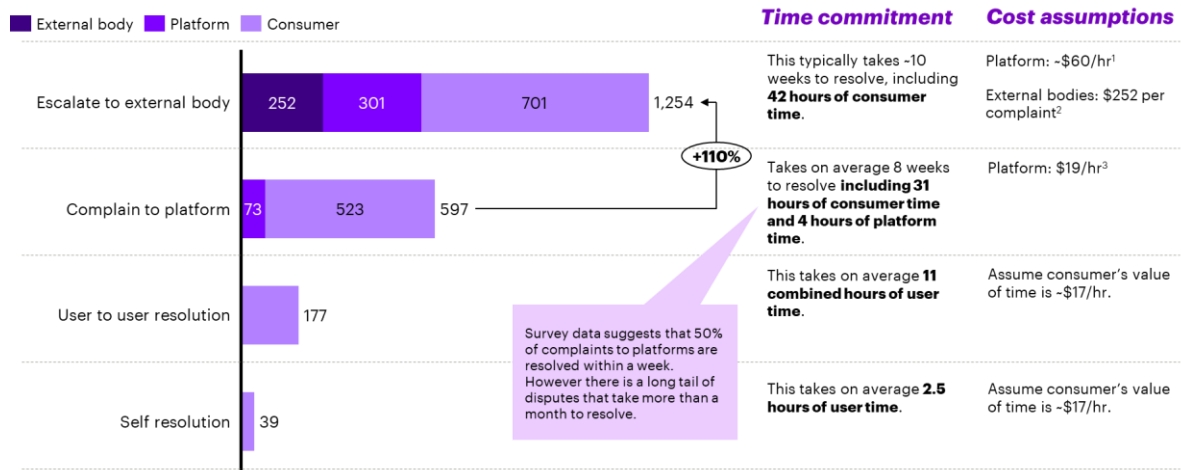
The costs to the different stakeholders of going through the issue, complaint or dispute process was calculated using survey and external data. For each resolution channel, costs of time and effort were determined for the consumer or business, the platform and the external body.

Exhibit 20 shows cost by channel per stakeholder for consumers in the bar chart, and on the right the assumptions around time commitment and costs. Here, it is seen that escalating to an external body has a total cost of \$1,254 per issue, complaint or dispute. The bulk of this cost is borne by the consumer (\$701), followed by the platform (\$301), followed by the external body (\$252). This is largely due to the function of time that each stakeholder spends trying to resolve the issue, with the consumer spending the most time. A comparable cost for businesses is also shown in **Exhibit 21**. Complaint costs for businesses will be higher than consumers as they are incurring wage costs.

Exhibit 20

The average cost of resolving a consumer issue, complaint or dispute varies widely depending on the resolution channel

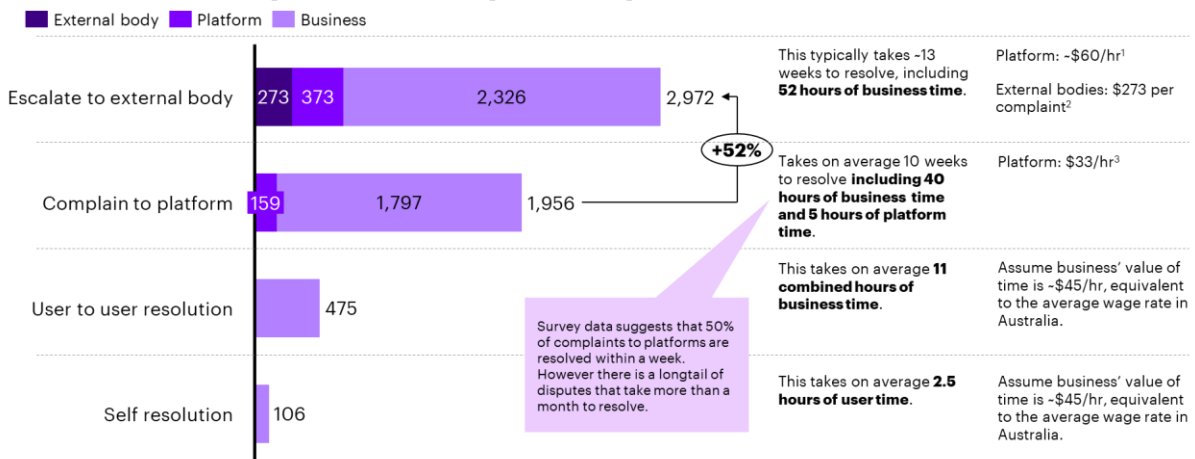
\$ cost of time and effort per user issue, complaint or dispute



Notes: (1) Wage of a legally trained professional who often becomes involved when the platform has to respond to a regulator. (2) We estimate the average cost per case using publicly available data on funding and the number of cases handled for different complaint-handling bodies. (3) Reflects the wages of subcontractors across the globe who are hired to review and moderate content. Source: Analysis of public data, information from external agencies and consumer and business survey. Cost to the platform for internal complaints is based on wage rates of complaint reviewers - these are often subcontractors working across the globe. Platform costs do not include costs of technology or infrastructure.

Exhibit 21**The average cost of resolving a business issue, complaint or dispute varies widely depending on the resolution channel**

\$ cost of time and effort per user issue, complaint or dispute



Notes: (1) Wage of a legally trained professional who often becomes involved when the platform has to respond to a regulator. (2) We estimate the average cost per case using publicly available data on funding and the number of cases handled for different complaint-handling bodies. (3) Reflects the wages of a platform customer service representative. Platforms will typically have a client account lead or customer service team specifically for businesses. Source: Analysis of public data, information from external agencies and consumer and business survey. Cost to the platform for internal complaints is based on wage rates of complaint reviewers - these are often subcontractors working across the globe

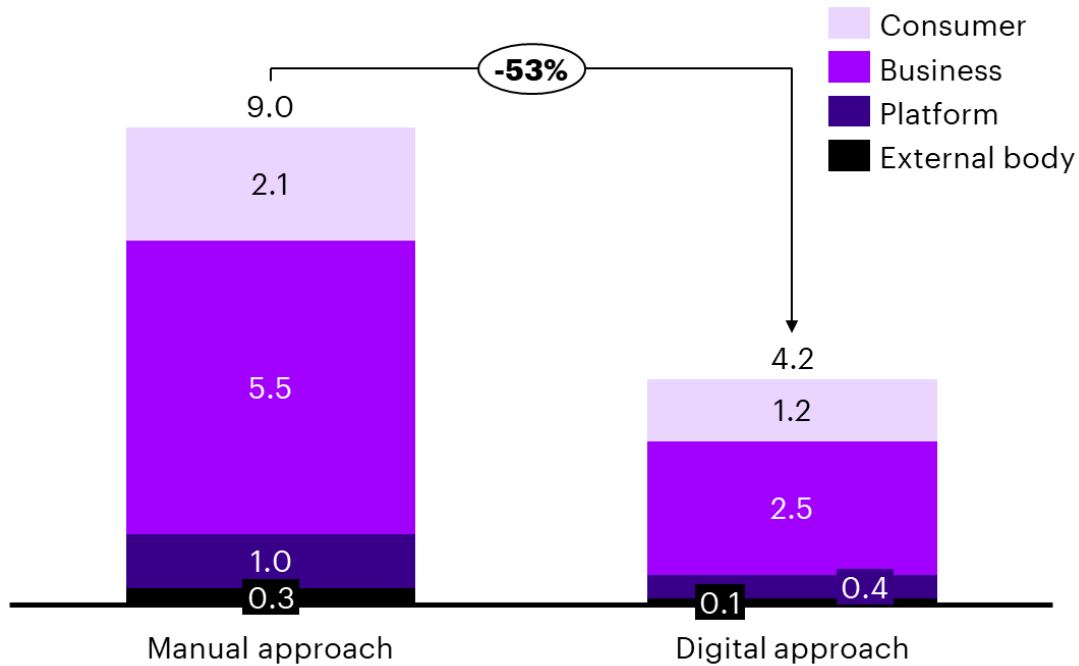
The innovative approaches taken by platforms has resulted in more efficient complaints handling

As shown previously in **Exhibit 13**, the digital platforms approach to issue, complaint and dispute resolution encompasses user-driven, platform-led and external dispute or escalation processes. Platforms take a preventative, scalable approach to resolving disputes. A focus on AI techniques to proactively identify problem actors, and a suite of user resources to self-resolve issues means they reduce the time and potential cost of dispute resolution.

Historically, goods and services not available on digital portals (e.g. landline phone services or banking before business websites became mainstream) used more manual channels to resolving an issue, complaint or dispute, such as raising it directly to the service provider or an external party.

In a thought experiment illustrated in **Exhibit 22**, the costs of resolving an issue, complaint or dispute via the digital platforms approach is compared to the cost of resolving an issue, complaint or dispute via a manual approach. The manual approach assumes that user-driven channels to resolve are not available (i.e., no self-resolve or user-to-user channels available), and therefore all those who would have raised the issue or complaint through that channel, have instead raised it directly with the platform.

The digital approaches taken by platforms has resulted in more efficient complaints handling, with costs being 50% lower compared to more a manual approach (\$4.2 billion compared with \$9 billion).

Exhibit 22**A digital approach to complaints and dispute management can cost half as much as manual approaches**Cost of managing user issues, complaints and disputes, \$b economic cost per year¹

Source: Analysis of public data, information from external agencies and consumer and business survey.

Notes: (1) This excludes the costs of capabilities that prevent issues

5. Pain points

The range of challenges that each platform faces can result in pain points for users

Although there are many advantages to addressing these issues in a digital environment, platforms must manage a range of challenges that are pertinent to the scale and nature of their service offering and digital business models. These challenges result in a number of pain points that users may experience, as **Exhibit 23** illustrates.

Exhibit 23

Users experience pain points due to challenges on digital platforms

Challenges faced by platforms	Resulting pain point
Handling the immense scale and scope of issues has led to the design of highly automated, scalable solutions	<ul style="list-style-type: none"> Bespoke or complex cases do not receive tailored solutions Users expect platforms to know them. Most disputes require proof of identity to resolve. Users know and accept that digital platforms already have a lot of information about them. They expect this information to be used to help resolve issues quickly, saving users from having to tell their story, and making it feel more personalised. Users are not always given the opportunity to speak with someone
Addressing a mix of complaints that differ in their complexity and severity makes it difficult to provide standardised approaches and resolution timelines	<ul style="list-style-type: none"> There is limited clarity on resolution timelines Users are unaware if their complaint has been actioned Complaints that are important to the user but low priority for the platform take extended periods of time to resolve (weeks if not months) Users are far more satisfied and confident that action is being taken when they understand the process. Even a few days feels like a lifetime to a user when they do not know what is happening and why it is taking time to resolve. Even if contact is limited and actions behind the scenes are not disclosed, those that understood the process had better experiences. Consumers expect rapid responses. Users expect the real-time, dynamic experience they have on platforms to translate to IDR. Many do not understand why issues need investigating, why time is required to resolve. They expect accounts to be reactivated and taken down immediately, money to be refunded instantly and reasons and decisions to be delivered swiftly.
Platforms feel that transparency of process, rules and decisions can lead to bad actors gaming the system and increase risk	<ul style="list-style-type: none"> Despite more clarity on the rules, users often do not get the reasons behind decisions and can lead to the perception that rules are not applied consistently Decisions and actions taken by platforms are unclear and confusing Leads some users to pursue external escalation Users often turn to community groups (both on and off the platform) to effectively resolve their issues or find out where to go next. No issue

	is unique and there are forums full of people willing to help. Informal action groups are used as workarounds, using the platforms reporting rules to achieve their desired outcome. A downside to these forums is that misinformation can occur.
Marketplaces need to balance consumer confidence and seller's needs	<ul style="list-style-type: none"> • Sellers may perceive a decision as biased towards the consumer and vice versa
Breadth of issues and platform products means no single agency ('one stop shop') to refer users for escalation	<ul style="list-style-type: none"> • Users are confused about where to go and how to resolve • There are many pathways for escalation • There is no sharing of complaint information between different complaint mechanisms (user has to tell their story twice)
Fake reviews can be subjective in nature and difficult for platforms to determine if they are fake	<ul style="list-style-type: none"> • Businesses can find it difficult to remove fake reviews • Fake reviews can remain 'live' for days and weeks before being removed (while platform investigates) which may lead to significant negative impacts on a business and their reputation.

Source: Interviews with platforms and users

One of the key pain points felt by consumers was limited transparency in cases where their content or account had been removed without an explanation or rationale. For example, when content has been blocked on Facebook, they will provide the community standard that has been violated, but not the specific content that violated that standard. Users can disagree with the decisions and Facebook will review the content within 24 hours (see **Exhibit 24**). Users typically receive strikes when they violate community standards which can ultimately lead to account removal depending on the severity of each violation. Platforms have identified that providing more details such as specific words or images, or the number of strikes, can enable people to 'game' the platform by using slightly different words, phrases or content so that their potentially offensive content is not detected. However, users have highlighted some frustration when little to no information has been provided about why their account or content was removed. In addition, users have highlighted cases where they have been bullied and multiple users have flagged their profile which led to their profile being removed, and unable to be recovered.²⁹ These examples are further detailed below.

Exhibit 24

Users can disagree with a decision when their content is removed

²⁹ Interviews with consumers and businesses

Source: Facebook <<https://transparency.fb.com/enforcement/taking-action/taking-down-violating-content/>>

Survey data shows that consumers were more likely to experience these pain points than businesses (see **Exhibit 25**). Some platforms indicated they had special customer service or client account teams for key business users of their platform.³⁰ s47G - business information

This may be why businesses in general had a better experience engaging with platforms. Additionally, some users are not paying 'customers' of platforms, and with vast user bases it is difficult to provide a tailored response.

Regarding the issue resolution experience, the top problems identified by consumers and businesses was that the platform did not direct them to other resources, closely followed by the platform not providing enough information or feedback. In both cases, there is a need for information and transparency for the user to help them resolve the issue and/or prevent it from happening in the future.

"Submitting a report felt like a shot in the dark – I had no idea if they'd got it or what was happening" – Interview with small business

³⁰ Interviews with digital platforms.

s47G - business information

"There was a huge form to fill out - you pour everything out, but you get nothing back" – Interview with consumer

"[Trying to dispute a decision] can feel like you're talking to a brick wall"
- Interview with small business

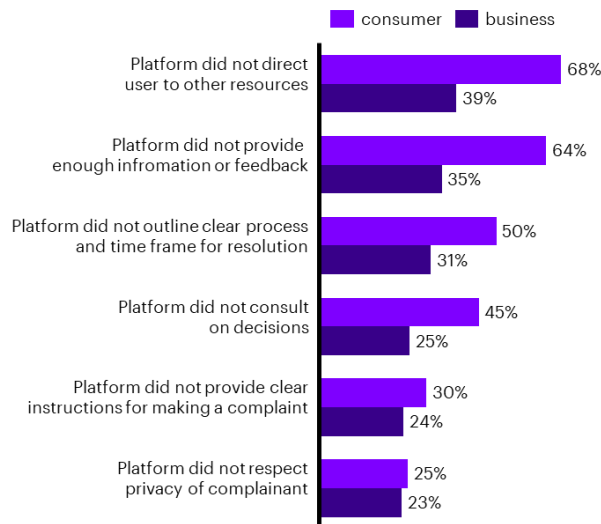
This aligns with the top two pain points felt by consumers; they found it difficult to contact someone and that the platform was not clear or transparent. For businesses, they also felt it was difficult to contact someone. In addition, they felt that the platform's actions were not consistent with the severity of the complaint. This last point highlights the differences in priorities that users and platforms face. Platforms may prioritise resources to issues, complaints and disputes which relate to crimes or break the law, or are experienced by paying customers, however for a small business, not being able to remove a fake review or recuperate a closed account can be detrimental to the business's success.

Exhibit 25

Consumers are more likely to experience pain points than businesses

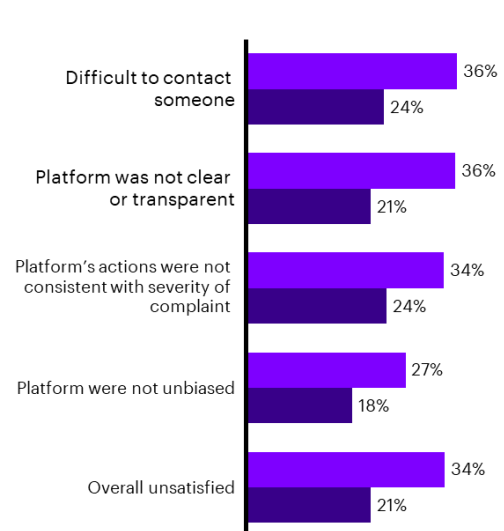
Key problems

% of users who complained to a platform



Key pain points

% of users who complained to platform



Source: Analysis of consumer and business survey

Users must navigate a complex ecosystem when trying to resolve their issue, complaint or dispute

In addition to the pain points that users sometimes face during the complaint handling journey, the dispute resolution ecosystem itself is composed of a vast mix of parties and systems, see **Exhibit 26**. This can make it hard for users to identify and speak to the best party that can help them resolve their issue. Digital platforms; government agencies and bodies; advocacy and consumer groups; the judicial system etc. can all provide some level of support to consumers and businesses who are trying to resolve a platform-related issue. Furthermore, complex complaints which may cover a lot of types of issues are difficult for a single agency to resolve.

However, each party or body often has limited jurisdiction or resources. Available assistance depends on the nature of the issue that the user is trying to resolve, sometimes the type of platform on which the issue occurred and whether the user is trying to seek action against a third party or the platform directly (see **Exhibit 9**).

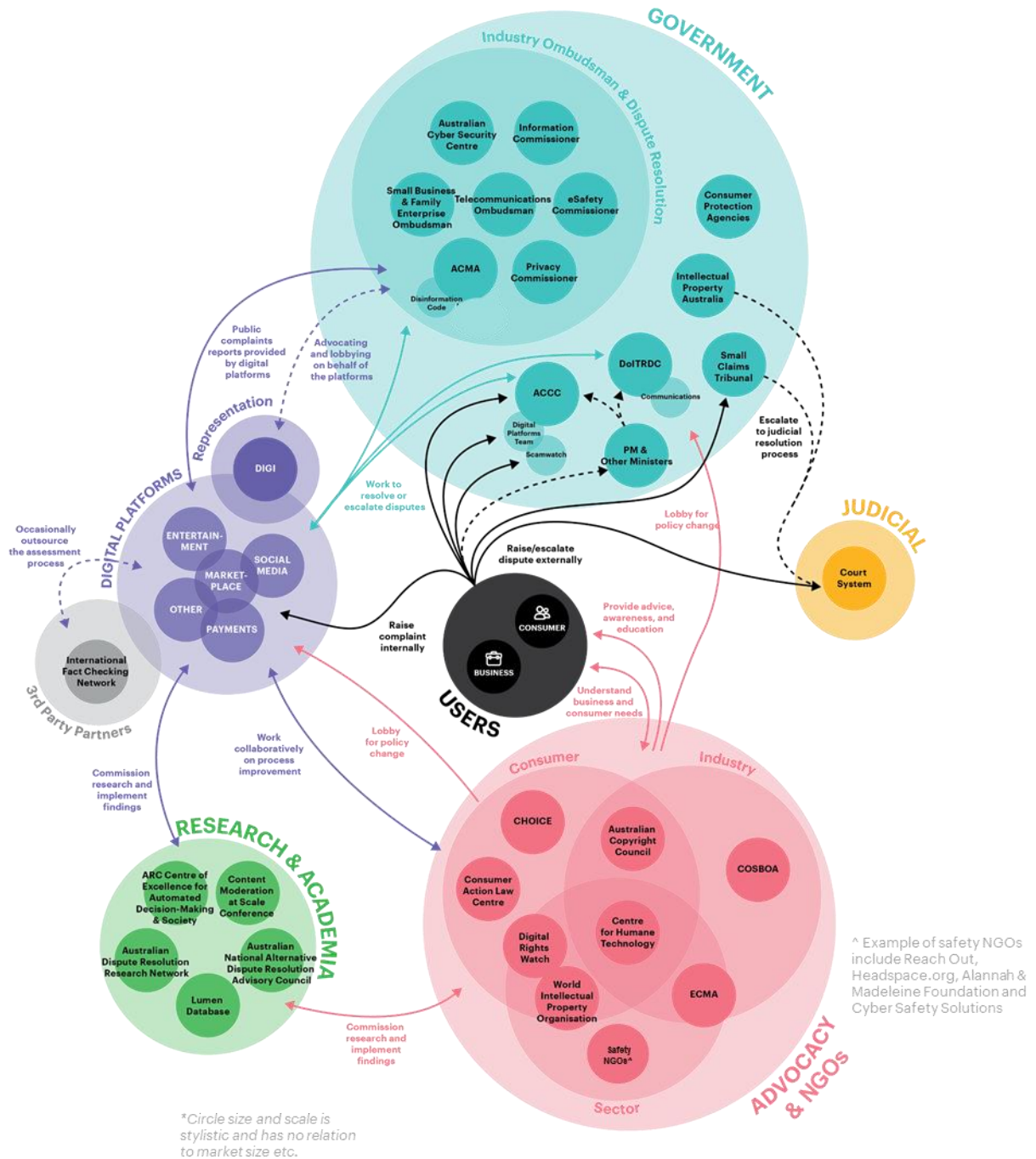
To lodge, investigate, escalate and resolve disputes, consumers and businesses often interact with a range of parties beyond the platforms themselves – all playing a critical but sometimes limited role in supporting the dispute resolution process.

There are many external bodies available to provide advice and assistance to users. However, the volume of players means consumers and businesses must navigate a relatively complex landscape with a potentially confusing number of dispute pathways.

Within the complex ecosystem, users can often be misdirected resulting in a drawn-out and frustrating path to resolution, as shown in **Exhibit 27**. Users can be misdirected across the three pathways of platform resolution, external escalation and judicial resolution and within a pathway (e.g. externally across agencies). At numerous points in the journey, generally after failing to resolve via one channel, a user must retell their story and provide details again.

Exhibit 26

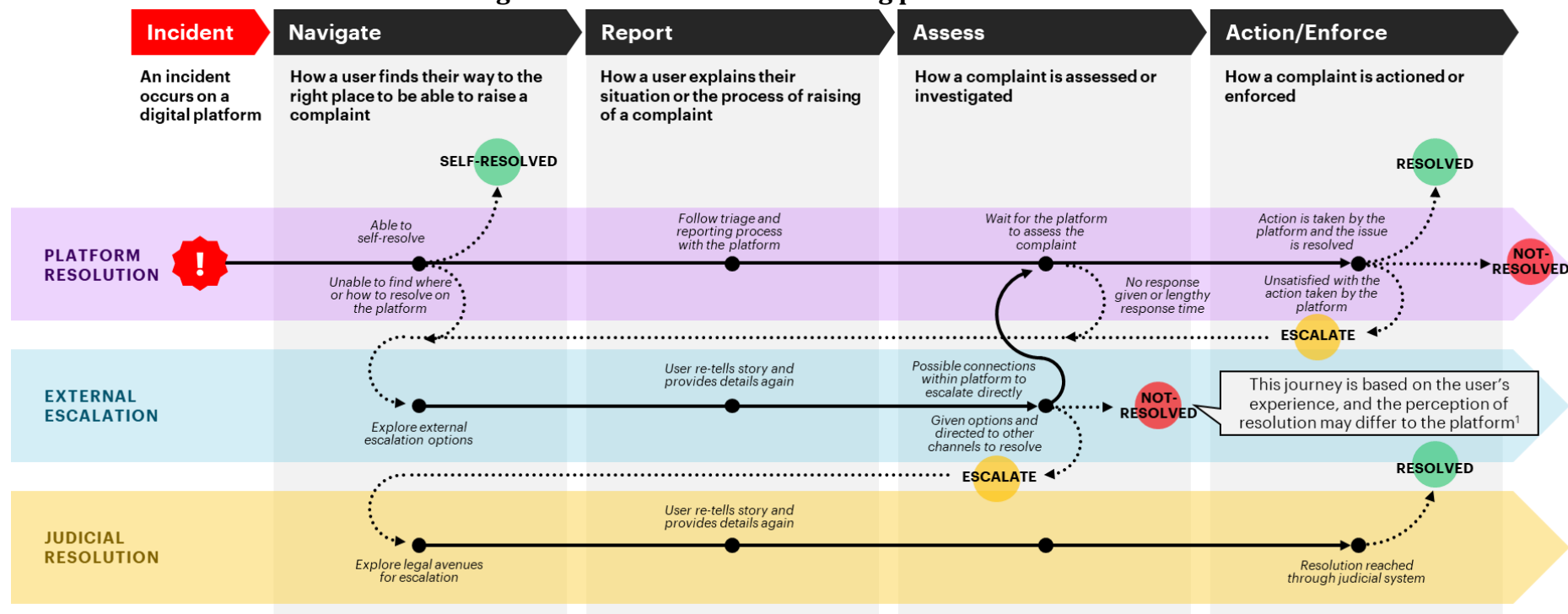
Users must navigate a complex ecosystem when attempting to resolve a dispute with external agencies



Source: desktop research, interviews with digital platforms, users regulators and government agencies

Exhibit 27

Users can often be misdirected resulting in a drawn-out and frustrating path to resolution



Source: desktop research, interviews with government agencies, information from platforms, analysis and synthesis of consumer interviews

Notes: (1) There are cases where the platform may have deemed the issue resolved and the user disagrees with this decision, which can result in dispute

To further illustrate user experiences, 15 ethnographic interviews were conducted to map different user experiences across the complaint and dispute resolution ecosystem.

One such user is Greg, a consumer whose experience is shown in **Exhibit 28**. Greg suddenly loses access to his social media accounts and is unable to stay connected to friends and family. Greg first attempts to resolve with platform resolution but is unable to and proceeds to escalate the matter externally. One of the key difficulties faced in this scenario is the lack of information and transparency from the platform regarding the reasons behind his account removal. Unfortunately, external bodies are only able to refer Greg back to the platform, where from Greg's perception, the issue remains unresolved. What Greg needed was reassurance from the platform that the issue could be resolved, and evidence and transparency from the platform to avoid the reoccurrence.

While the issue remains unresolved for Greg, the process showcases some positive points. For example, the platform was able to provide an easy step-by-step process to complete a dispute account closure form, and even though the external agency could not help Greg, Greg was able to receive advice and assistance in preparing the right documentation to take back to the platform.

Another user is Chloe, a small business owner who has had several misleading and information reviews posted about her business. Her experience is illustrated in **Exhibit 29**.

In Chloe's case, a first attempt to resolve using user-to-user resolution on the platform does not yield results. Chloe's second attempt is to go directly to the platform, by reporting the other user's profile via a 'report' link on their profile. She then follows a step-by-step questionnaire, and the platform resolves the issue within two days.

Chloe needed a swift resolution to minimise damage to the credibility and reputation of her business and certainty of resolution. The platform's intuitive in-situ reporting methods, step-by-step process, confirmation that an investigation is on the way, and the provision of an alternate contact number gave Chloe the tools, reassurance and resolution she needed to protect her business.

Exhibit 28

Greg's experience as a consumer demonstrates the pain points across the journey

GREG

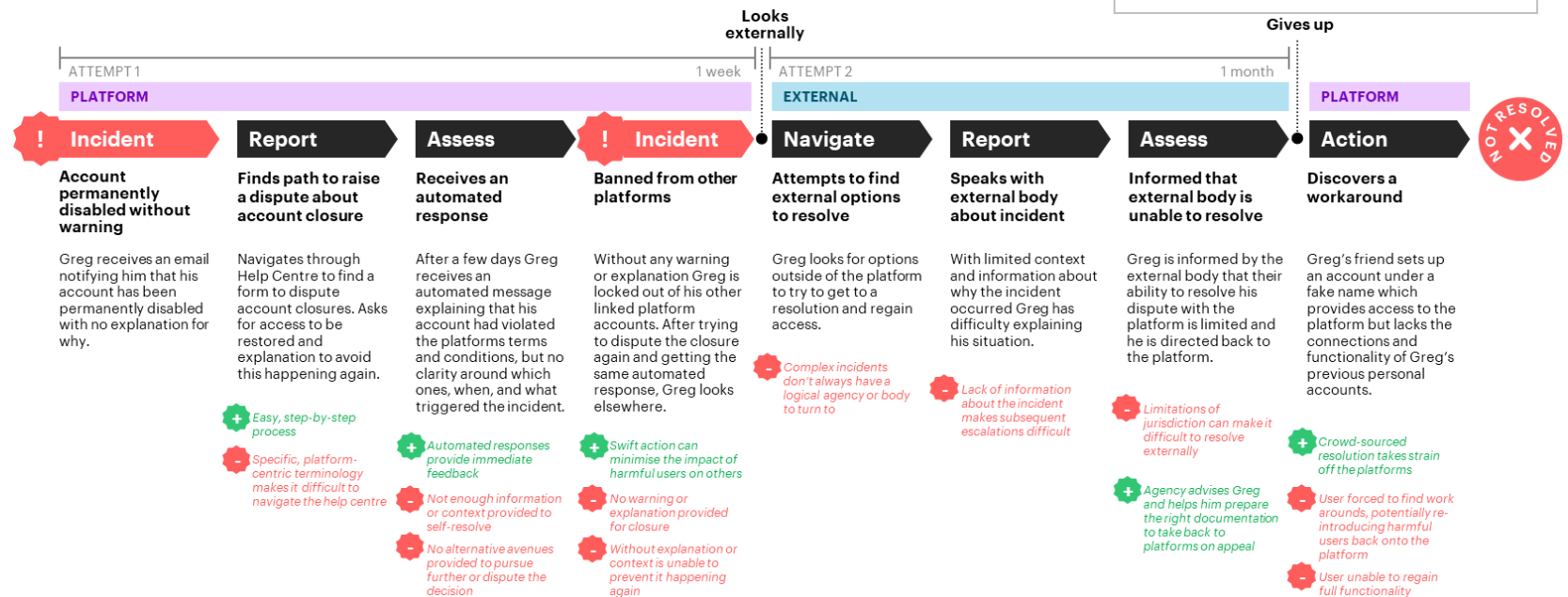
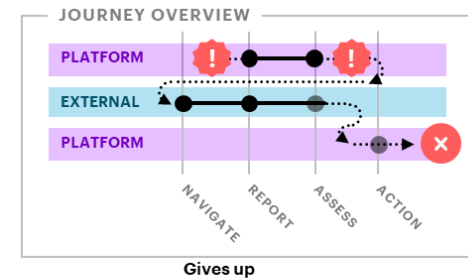


CONTEXT

Greg suddenly loses access to his social media accounts and is unable to stay connected to friends and family

NEEDS

- Reassurance that the incident can be resolved
- Evidence and transparency from platform to avoid reoccurrence



Source: Ethnographic interviews

Exhibit 29

Chloe's experience shows a stepwise process for businesses dealing with fake reviews

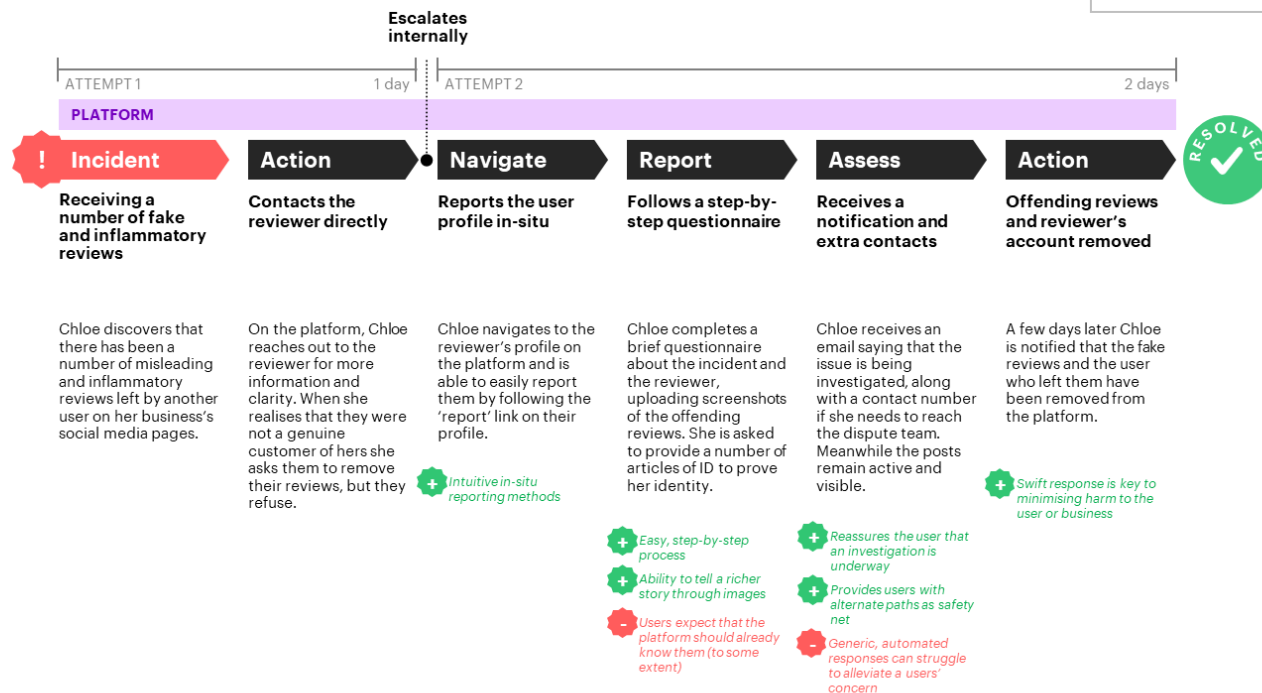


CONTEXT

Chloe is a small business owner who has had a number of misleading and inflammatory reviews posted about her business.

NEEDS

- A swift resolution to minimise damage to the credibility and reputation of her business
- Ability to prevent this recurring
- Certainty of resolution



Source: Ethnographic interviews

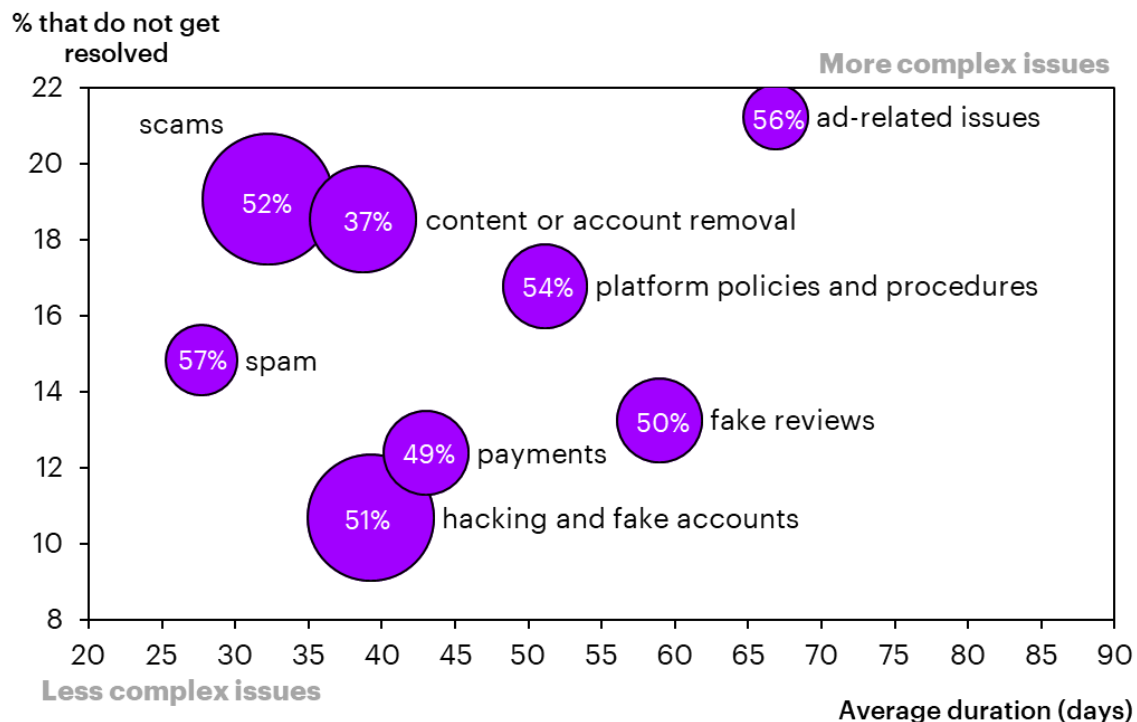
While platform resolutions are adapted to scalability and efficiency, they may be limited when it comes to managing more complex complaints

Some complaint types are better suited than others for the platform resolution process. The chart below shows that resolutions can be quickly achieved for easy issues, such as hacking and fake accounts, payments, spam, and scams.

Exhibit 30

Platform resolutions are adapted to scalability and efficiency, which may be unsuited to resolving more complex complaints

Size of bubble is number of issues, complaints or disputes. Percentage in bubble is the share of users who said they were satisfied with the platform's complaint process.



Source: Analysis of consumer and business survey

Uncontroversial, high volume complaints such as hacking and fake accounts are generally resolved using algorithmic/AI techniques that identify and remove these accounts or flag them for human review. Hacked and fake accounts that are experienced by users generally have lower duration to resolution because they are quickly identified by users (e.g. the account starts to post ads) and are relatively straightforward to resolve (e.g. provision and verification of ID documents).

While many platforms use algorithmic approaches to remove content or accounts, these issues are often more subjective. Contentious removals often fall through the speedy, rules-based resolution of platforms and lead to a higher number of unresolved issues.

With platforms having several in-situ features to flag or report spam, these types of issues tend to have a shorter duration.

Ad-related issues for business and fake reviews are often only resolved by directly contacting the platform. Some platforms provide more traditional customer service to business users. This hands-on

approach means issues take longer to resolve. More subjective ad-related issues, such as an ad not delivering expected results, are also less likely to achieve a resolution.

"It was long process that took repeated effort and lots of information to get an answer."

- Interview with small business regarding an advertising issue

This leads to a higher number of disputes where an automated or self-guided system is unable to deliver a resolution

Complex complaints lead to a higher number of disputes. The chart on the left-hand side of **Exhibit 31**, 'Complaints by resolution', shows the proportion of resolved issues, complaints and disputes, including those that are not resolved at all. Most are resolved as issues (38%) or complaints (26%), while 36% are resolved as internal disputes with the platform, external escalation with a third party, or not resolved at all.

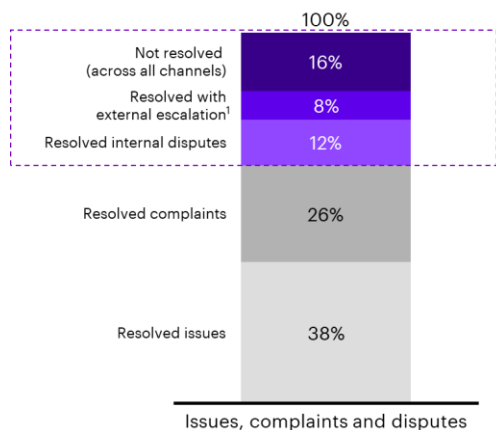
The numbers in the below chart are comparable with the TIO annual report figures, which show that the proportion of unresolved complaints to the TIO by issue type can range from 9 to 19% in 2019-20.³²

Exhibit 31

There tends to be a higher rate of disputes for complaint types that are less suited to automated and self-guided solutions

Complaints by resolution

% of total issues



Disputes and unresolved issues

% of issues that are disputes and unresolved by complaint type



Source: Analysis of consumer and business survey

Notes: (1) Includes external disputes and external escalation

The chart on the right-hand side of **Exhibit 31** takes a closer look by complaint type at the 36% of resolved internal disputes, external escalation and not resolved. For example, for content or account removal complaint type, it can be seen that 17% are resolved through internal dispute with the platform, 11% are resolved with external escalation to a third party and 19% are not resolved at all. For this complaint type, there is a higher dispute and unresolved rate because platforms do not tend to reveal the reasons why content or accounts have been removed. Platforms have highlighted that this can occur to prevent bad actors from gaming algorithms.

³² Telecommunications Industry Ombudsman [Annual Report](#) 2019-2020

Platform policies and procedures have a higher chance of leading to a dispute. These are issues that users cannot resolve on their own and must be raised directly with a platform.

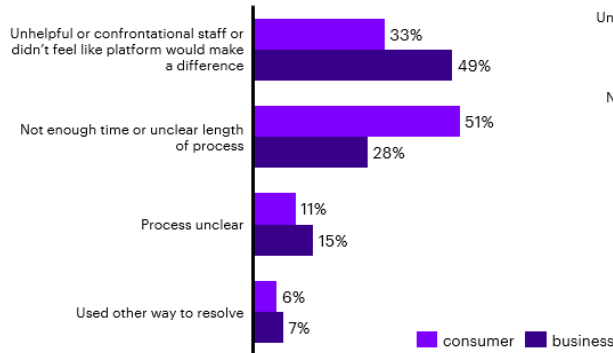
Ad-related issues (21%) and scams (19%) have a higher percentage of unresolved matters. More subjective ad issues like an ad not delivering expected results are less likely to end in a resolution. One reason for an ad not delivering on its expected result could be due to unexplained and sudden changes in ad algorithms. Changes in ad algorithms account for almost 50% of the reported ad-related issues across the platform types.

While platforms are generally good at removing or down-ranking scam content, the high proportion of unresolved issues could be because the users who are victims of more severe scams may want further redress which platforms are not able to provide. Similarly, with external agencies, their mechanisms only allow for reporting of scams, which may help flag offenders and have them removed but not necessarily compensate individual victims of scams.

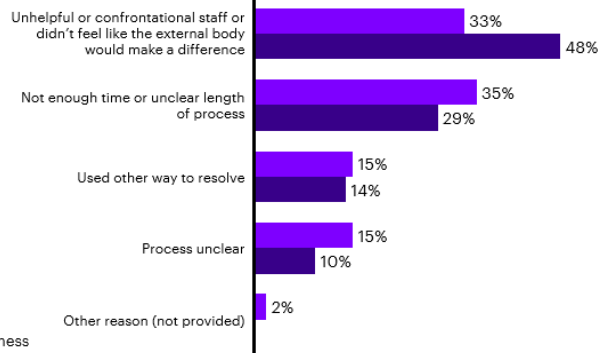
Unresolved issues are comprised of cases where an issue was ongoing and the user is unsatisfied (49%) or when they have withdrawn their complaint (51%). **Exhibit 32** shows the reasons why consumers and businesses withdrew from the platform or an external dispute process. The main reason why users withdrew from either an external body or platform was that they believed the staff or process to resolve was not helpful, or unlikely to change the outcome. Lacking the time to be able to resolve the complaint or unclear processes was also a major reason for withdrawing.

Exhibit 32**Half of the unresolved issues, complaints and disputes were due to users withdrawing from platforms or external agencies****Withdrawals from platforms**

% of respondents who withdrew complaint or dispute from platform

**Withdrawals from external escalation**

% of respondents who withdrew from external escalation



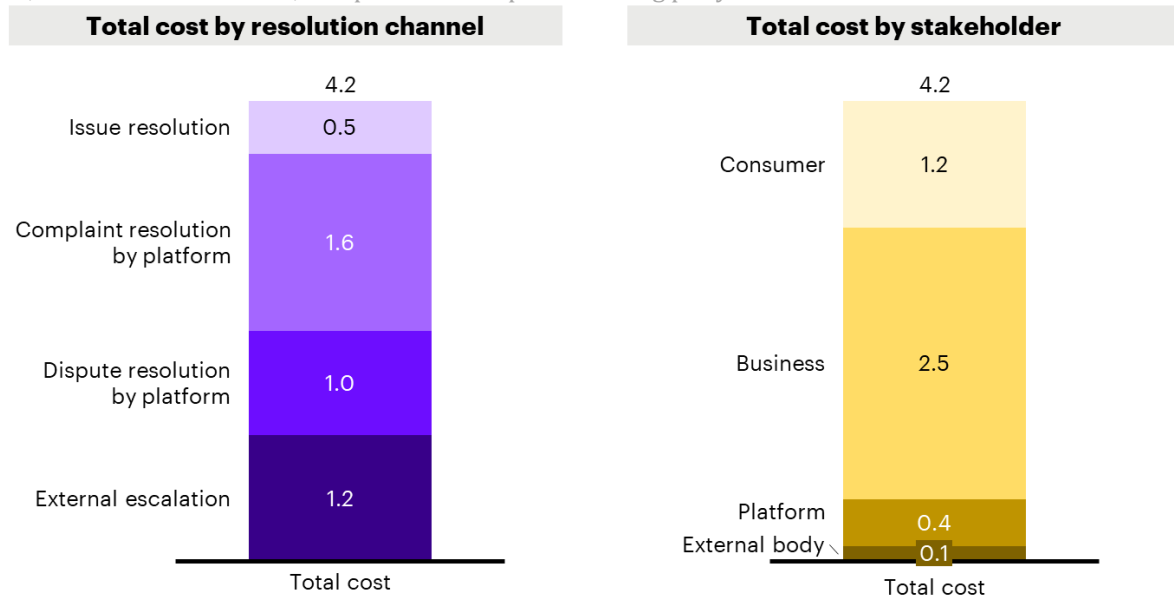
Source: Based on survey results for consumers and businesses who made a complaint to a third party or platform and withdrew their complaint

The more complex issues that result in a complaint and dispute place a higher cost for platforms, agencies and users

Exhibit 33 shows the total cost in one year of handling the total number of platform-related issues, complaints or disputes by resolution channel (left-hand side chart) and stakeholder (right-hand side chart). The current digital dispute resolution processes cost the economy \$4.2 billion in time and effort associated with resolving issues, complaints and disputes. Of which the majority (\$3.7 billion) is the cost to users and businesses.

Exhibit 33**The economic cost of responding to and handling issues, complaints and disputes on digital platforms is \$4.2 billion annually**

\$b, economic cost of issue, complaint and dispute handling per year



Source: Analysis of public data, information from external agencies and consumer and business survey. Note: excludes the economic cost of any harm or consequence as a result of the subject matter of the complaint and not the complaint handling process.

The largest cost points in the current system come from handling platform complaints and external escalations. The large cost of platform complaints is primarily due to the high volume of issues that lead to a platform complaint. In 2020, 60% of issues resulted in a platform complaint (see **Exhibit 15**). Only 11% of issues resulted in an external escalation yet these account for 27% of the total cost. This is due to the difficulties and misdirection that users experience in navigating the external escalation environment, as well as the increased likelihood that more complex cases result in external escalation.

Currently, the costs in the system are borne largely by consumers and businesses. The cost borne by external bodies is small, even though the cost of handling external escalations is high (see chart on left). This is because while external escalations will involve consumers, businesses and platforms, most of the time spent in addressing external complaints is by users and businesses (e.g. gathering information, retelling story) leading to most of the cost being borne by consumers and business.

The greatest consequence of the complaint nature or resolution process was lost time and effort for consumers, and reputational damage for businesses

In addition to the individual cost of resolving an issue, complaint or dispute (see **Exhibit 20**), consumers and businesses experience other losses. **Exhibit 34** lists the range of adverse consequences from the complaint nature or resolution process for consumers and businesses.

Exhibit 34

Users experienced lost time and effort, financial losses, reputational damage and other impacts as a result of issues, complaints and disputes

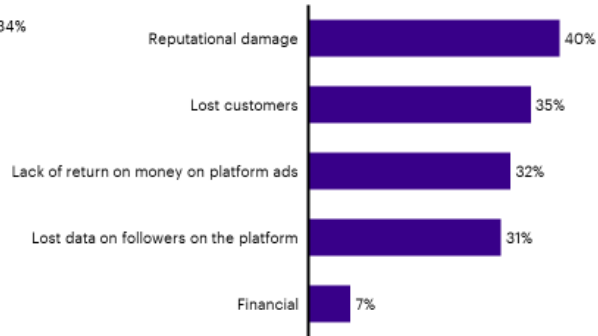
Consumer adverse consequences from complaints

% of consumers



Business adverse consequences from complaints

% of businesses



Source: Analysis of consumer and business survey

(3.) Calculations for lost business tax revenue is based on the ratio of business tax revenue to business income as reported in ABS taxation revenue and Australian industry releases.

Overall, businesses are more likely to experience adverse consequences. This could be because more is at stake for businesses in their complaints as digital platforms can be critical for their marketing and sales.

2 in 5 businesses incurred reputational damage as a result of a platform-related issue. Of those that reported a financial loss, the average amount was \$8,855. This equates to \$101 million across all SMBs in 2020 and \$2.5 million in lost business tax revenue.³³

The impact of platform-related issues on consumers ranged from lost time, mental health impacts, lost connections and in some cases even losing their job. Of those consumers who reported a financial loss, the average amount was \$1,353. This equates to \$87 million across the population in 2020.

³³ Calculations for lost business tax revenue is based on the ratio of business tax revenue to business income as reported in [ABS taxation revenue](#) and [Australian industry releases](#)

s47C - deliberative processes



³⁴ Twitter 2021, Q1 2021 [Letter to Shareholders](#)

s47C - deliberative processes



s47C - deliberative processes



A.Appendix

Exhibit 37

Agency	How do they support external escalation?	What are their limitations?
ACCC	The ACCC can provide information about consumer rights and obligations and potential courses of action to resolve a dispute. ³⁵ They can also undertake investigations and take enforcement action where there are systemic issues, serious breaches of the law or abuses of market power.	The ACCC do not arbitrate, mediate or resolve individual's complaints. ³⁶ As a result, consumers may be unlikely to contact the ACCC, making it difficult for the ACCC to get a true picture of the scale, scope and sufficient detail of issues being faced by individual or small business consumers.
ACCC - Scamwatch	Scamwatch is run by the ACCC It provides information to consumers and small businesses about how to recognise, avoid and report scams. The purpose of Scamwatch is to help individuals and the community recognise scams and avoid them. The ACCC works with state and territory consumer protection agencies and other government agencies to promote awareness in the community about scams.	The ACCC's Scamwatch does not give legal advice and is unable to offer assistance in individual cases or to investigate each scam. ³⁷
AFCA	AFCA takes complaints about entities with a financial services licence, e.g. banks, superannuation companies, insurance firms, mortgage brokers and financial planners. ³⁸ AFCA may use a range of methods to reach a resolution including negotiation, conciliation, preliminary assessment or a binding determination.	AFCA can receive complaints about digital services platforms that have a financial services license (e.g. Afterpay). Consumers can only complain to AFCA if the complaint relates to the conduct of a licensed financial services entity on a digital services platform but then the complaint must relate to the licensed entity rather than the platform.
ACMA	ACMA take consumer complaints about breaches of the Spam Rules. After reviewing a complaint, ACMA may contact the sender about their responsibilities under the Spam Rules. If the issue is serious or ongoing, then ACMA may investigate the complaint. ³⁹ Where ACMA finds that the law has been broken it may: <ul style="list-style-type: none"> • take the matter to the Federal Court, which can impose significant penalties • give an infringement notice • issue a formal warning • accept court-enforceable undertakings.⁴⁰ 	Under s.9 of the <i>Spam Act</i> , liability rests with the entity who authorised the sending of the message (spam) rather than the carriage service provider, including internet carriage services.

³⁵ <https://www.accc.gov.au/consumers/consumer-protection/where-to-go-for-consumer-help>

³⁶ <https://www.accc.gov.au/consumers/consumer-protection/where-to-go-for-consumer-help>

³⁷ Scamwatch, 'About Scamwatch', < <https://www.scamwatch.gov.au/about-scamwatch/scamwatch-role> >

³⁸ <https://www.afca.org.au/make-a-complaint>

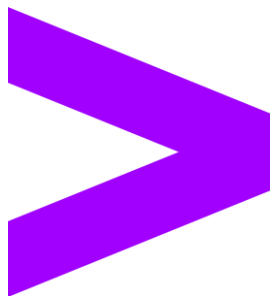
³⁹ <https://www.acma.gov.au/stop-getting-spam>

⁴⁰ <https://www.acma.gov.au/investigations-spam-and-telemarketing>

ASBFEO	<p>ASBFEO will assist small businesses to resolve a dispute (defined as <100 employees, <\$5m revenue in the previous financial year in s.5 of the <i>Australian Small Business and Family Enterprise Ombudsman Act 2015</i> ('ASBFEO Act')). This assistance offered by the ASBFEO may include referring the dispute to the appropriate Federal, State or Territory agency (s.15(a) and making recommendations on the management of the dispute including making a recommendation that an external ADR process be used (s15(b)). They also support small businesses by helping to triage their complaint and gather the appropriate information.</p>	<p>ASBFEO do not have jurisdiction to resolve the dispute themselves and cannot compel the parties to enter into ADR. Indeed, under s.73(2) of the ASBFEO Act, "An alternative dispute resolution process recommended by the Ombudsman must not be conducted by:</p> <ul style="list-style-type: none"> (a) the Ombudsman; or (b) a delegate of the Ombudsman; or (c) a person assisting the Ombudsman under section 33; or (d) a person engaged as a consultant under section 34."
OAIC	<p>The Office of the Information Commissioner can investigate complaints about the mishandling of an individuals' personal information in potential breach of the <i>Privacy Act 1998</i> (Cth). The <i>Privacy Act</i> applies to all organisations with an annual turnover in excess of \$3m, with limited exceptions covering some small businesses with turnover under this amount. When the OAIC receives a complaint, they may decide to investigate the complaint themselves or refer the complaint to another external dispute resolution body (usually a sectoral industry ombudsman where one exists). Where the OAIC investigates a complaint themselves and finds that there has been a breach of the <i>Privacy Act</i>, they are empowered under the Act to seek either a conciliated outcome or to make a binding determination.</p> <p>Possible outcomes of an upheld complaint include remedying the matter, an apology, training, changes to policy or procedures, compensation for financial and non-financial losses or enforceable undertakings. In the case of severe breaches of privacy, a civil penalty may be sought.</p>	<p>The Australian Privacy Principles protect individuals' personal information and privacy, rather than that of small businesses.</p>
State-based Small Business commissioners	<p>The various State Small Business Commissioners offer mediation services to help resolve complaints between a small business and another business. These services commonly resolve disputes about retail leases, general commercial leases, bonds or business contracts. Both parties must consent to going to the mediation service provided by the Small Business Commissioner. For example, the NSW Small Business Commissioner can receive and deal with complaints where the subject matter relates to unfair treatment of, or unfair practice involving, the small business, or an unfair contract to which the small business is party, or it is in the public interest to deal with the complaint (s 14 Small Business Commissioner Act 2013). The NSW Small Business Commissioner resolves 90% of disputes referred to its mediation service.</p>	<p>If the parties cannot reach an outcome acceptable to them both via mediation, then a party may elect to have the matter heard by the relevant court or tribunal.</p>
State-based consumer affairs or fair trading (ACL regulator)	<p>Individuals and small businesses can make a complaint to their State or Territory Consumer Affairs or Fair-Trading Agency if they believe there has been a breach of the ACL. Parties are encouraged to resolve the matter between themselves prior to a referral to an ACL regulator. Once a complaint has been accepted by an ACL regulator, the parties will</p>	<p>If either party does not agree to the outcome, and a binding decision is required or the outcome needs to be enforced, the parties may then need to go to Court or the relevant consumer tribunal.</p>

	<p>go through a conciliation process in an effort to reach an acceptable outcome. These regulators also have investigation powers and where they find that there has been a serious or systemic breach of the Australian Consumer Law, they may seek additional remedies such as prosecution, civil penalties, injunctions or enforceable undertakings.</p>	<p>An ACL regulator is less likely to pursue matters that: are one-off, isolated events; involve contraventions that are technical in nature; are more appropriately resolved directly between the parties under an industry code (for example, by mediation or an industry dispute resolution body); are more appropriately dealt with under jurisdiction-specific legislation; involve issues more effectively dealt with by another agency, or are best dealt with between the parties (the ACL provides complainants with a private right of action in these circumstances)."⁴¹</p> <p>The consumer guarantees contained in the ACL only apply to those goods or services under \$100,000 from 1 July 2021, or those over \$100,000 normally purchased for personal or household use, which limit their application for the benefit of small businesses.</p>
<p>Australian Cyber Security Centre</p>	<p>The Australian Cyber Security Centre acts as a clearing house for reports about cybercrime, specifically those crimes relating to identity theft and fraud, online fraud, cyber-enabled abuse, online image abuse and affected devices. Those reports are referred to the relevant State or Federal police agency for assessment.</p>	<p>The Australian Cyber Security Centre accepts reports from both individuals and small businesses however, they do not investigate the complaints themselves.</p>

⁴¹ <https://www.consumer.vic.gov.au/library/publications/businesses/fair-trading/compliance-and-enforcement-acl-guide-word.doc>





Australian Government

Department of Infrastructure, Transport,
Regional Development and Communications

Summary of Existing External Escalation Ecosystem

Advisory Panel Meeting Paper 2

July 2021

As part of its feasibility study, DITRDC is examining the functions and powers of existing external bodies. These include:

- Australian Competition and Consumer Commission (ACCC);
- State and territory consumer protection bodies;
- Australian Small Business and Family Enterprise Ombudsman (ASBFEO);
- Australian Communications and Media Authority (ACMA);
- State Small Business Commissions;
- Australian Cyber Security Centre (ACSC);
- Council of Small Business Organisations Australia (COSBOA);
- Office of the eSafety Commissioner; and
- Office of the Australian Information Commissioner (OAIC).

These bodies are being examined because their remit includes or is related to in-scope issues experienced either by individuals or small businesses that use digital platforms. Descriptions of in-scope issues are provided below in Table 1. In its research, Accenture has identified many of these bodies as forming part of the existing ecosystem of possible external escalation pathways available to users of digital platforms.

This Paper does not provide exhaustive descriptions of the remits and powers of the bodies described above. DITRDC is seeking input from Panel members on the content of this paper by Monday, 9 August 2021.

Questions for Advisory Panel members

- Do the below summaries and Table 2 provide an accurate representation of your body's authority to deal with in-scope issues, and its powers to assist with the resolution of those issues?
- For in-scope issues within your agency's remit, do you have powers to assist in resolving those issues that you do not currently exercise? If yes, what are the reasons for not exercising these powers (e.g. lack of resources; unclear about whether your agency's powers can apply to digital platforms, particularly those based overseas)?
- What types of in-scope digital platform issues do you currently receive complaints about?
- What methods do you currently use to resolve these complaints (including formal powers or informal relationships)?
- Are there additional bodies to those identified that deal with in-scope digital platform issues, and that may have powers to resolve those issues?

Table 1 In-scope issues

In-Scope Issue	Description
Payment and transaction issues between users	<i>Payment and transaction issues between users, on a platform that has a payment system or functions as a marketplace.</i>
Spam	<i>Content that is unsolicited, annoying and usually posted or sent in bulk to users.</i>
Scams	<i>Content that is false and designed to trick users into spending money, sharing their personal information etc. Includes online shopping, investment, dating scams, fake ads and phishing.</i>
Fake reviews	<i>Fake reviews or comments e.g. fake reviews on a business page to boost sales, or fake, vexatious complaints received from unsatisfied customers.</i>
Hacking and fake accounts	<i>Account hacking or fake accounts created to mimic another user, or fake accounts created to engage in offensive or inauthentic behaviour.</i>
Account and content removal	<i>When a platform suspends or removes an account, or removes content posted by a user. For businesses this can result in loss of followers or customer data on the platform.</i>
Ad-related issues	<i>Issues around ads such as being incorrectly billed for an ad, ad not delivering promised or expected results, transparency around ad effectiveness and unexpected changes to platform algorithms that reduce ad visibility.</i>
Issues around platforms' complaint handling policies and procedures	<i>Issues that users have with the platform's complaint handling policies and processes. Examples include where users couldn't find information on how to make a complaint or contact the platform and where users were told they were in breach of platform guidelines but didn't know which provision.</i>

Australian Consumer Law (ACL) Regulators

The Australian Consumer Law (ACL), contained in Schedule 2 of the Competition and Consumer Act 2010 ('CCA'), is the primary mechanism through which Australian consumer rights are safeguarded.

The ACL is enforced by federal, state and territory ACL regulators. At the federal level, the ACCC is the main regulator, while the Australian Securities and Investment Commission (ASIC) regulates financial products and services. Each state and territory has its own consumer protection body. Each regulator is independent, has its own enabling legislation and exercises its powers and functions in accordance with that legislation.

For in-scope digital platform issues, these regulators would only have powers to assist if they believe an issue constitutes a breach of the ACL (or the CCA more broadly for the ACCC). The ACL regulators cannot make a decision as to whether a person or business has breached the law, this must be determined by a court. While some issues may be better pursued as private actions, such as payment issues between two users, many of the in-scope issues may stem from conduct which is prohibited under the ACL and which could be resolved by enforcement action by ACL regulators.

ACL regulators have a number of compliance and enforcement powers open to them, which could be employed in response to all complaints from consumers about breaches of the law. However, in practice these are reserved for significant and systemic breaches. This is largely due to the resource intensive nature of bringing court action, as is required to determine whether breaches have occurred.

Australian Small Business and Family Enterprise Ombudsman

In exercising its assistance function, the ASBFEO has the power to respond to requests for assistance by small businesses and family enterprises (SBFEs), in relation to “relevant actions”. “Relevant actions” are actions (activities, projects, making a decision or recommendation, or an alteration of, failure or refusal to do any of those things) by an entity that affects, or may affect, a SBFE in the course of trade or commerce between Australia and places outside Australia, or within Australia. ASBFEO may have authority to assist with any in-scope issue, where the “action” of an entity affects a small business in trade or commerce.

The ASBFEO has the power to make recommendations about how a dispute about relevant actions may be managed, including recommending that an alternative dispute resolution (ADR) process be used.¹ In practice, the ASBFEO firstly provides information on how to resolve disputes and facilitates discussions between disputing parties. This requires the ASBFEO to locate a platform contact. If the dispute is not resolved at this stage, the ASBFEO can refer SMFEs to an appropriate ADR process.² ADR processes are defined to include mediation, conciliation, conferencing, case appraisal and neutral evaluation. They do not include court procedures or arbitration.³

Australian Communications and Media Authority

ACMA is the federal government regulator for communications and media. It is an independent Commonwealth statutory authority, established by the Australian Communications and Media Authority Act 2005 (‘ACMA Act’). Of the functions conferred by the ACMA Act and other relevant legislation, the only functions that relate to an in-scope digital platform issue are those conferred under the Spam Act 2003 (‘Spam Act’).

Users can make a complaint about spam to ACMA, following which ACMA may contact the sender about their responsibilities under the Spam Act and may investigate serious or ongoing issues. ACMA also has a range of enforcement options open to it for breaches of the civil penalty provisions of the Spam Act. These include injunctions, enforceable undertakings, and formal warnings.⁴ It is important to note that the Spam Act is concerned with the sender of spam messages, rather than the platform on which it is sent. Therefore, investigations or enforcement action would be against the user who sent the message.

People can also report spam to ACMA, which does not register as a complaint but allows ACMA to identify spam trends and potential compliance issues.

State Small Business Commissions

Some states have independent statutory bodies that offer dispute resolution services to small businesses. These include:

- Victorian Small Business Commission
- New South Wales Small Business Commissioner
- Western Australia Small Business Development Corporation
- South Australian Office of the Small Business Commissioner

Their functions and powers are different and defined by each body’s establishing legislation. For example, the Victorian Small Business Commission has authority to receive complaints by Victorian small businesses about unfair market practices or commercial dealings, and to provide alternative dispute resolution (ADR) to the parties involved.⁵ It can also

¹ ASBFEO Act s 71.

² [How we help | Australian Small Business and Family Enterprise Ombudsman \(asbfeo.gov.au\)](#)

³ ASBFEO Act s 4.

⁴ Spam Act 2003 pts 4–7.

⁵ *Small Business Commission Act 2017* (Vic) s 5.

provide ADR to small businesses involved in any “disputes”, defined to include a contractual or commercial dispute between a small business and another business.⁶ ADR in this context includes mediation and preliminary assistance.⁷

Australian Cyber Security Centre

The Australian Cyber Security Centre (ACSC) is part of the Australian Signals Directorate, a Commonwealth statutory agency within the Department of Defence portfolio. It receives reports of cybercrime, and refers these reports to the appropriate police jurisdiction for assessment. Some in-scope issues may amount to cybercrimes, such as if scams or hacking and fake accounts amount to online fraud or identity theft. The ACSC has no power to resolve disputes itself.

Council of Small Business Organisations Australia

The Council of Small Business Organisations Australia (COSBOA) is the peak industry body representing the interests of Australian small businesses. It performs advocacy functions, however it has no formal powers to assist in the resolution of disputes and does not provide informal assistance for individual disputes.

Office of the eSafety Commissioner

The eSafety Commissioner was established as an independent statutory office under the Enhancing online Safety Act 2015 (Cth). It currently deals only with out-of-scope issues; however, the Online Safety Bill 2021 (Cth) includes powers for the Minister for Communications to determine Basic Online Safety Expectations. These could include additional Expectations that cover in-scope issues.

Office of the Australian Information Commissioner

The Office of the Australian Information Commissioner deals with issues that fall out of the scope of this project.

Table 2 below provides a summary of the authority of existing external bodies to deal with in-scope issues, and whether they have any powers to assist with the resolution of those issues.

⁶ *Small Business Commission Act 2017* (Vic) s 5.

⁷ *Small Business Commission Act 2017* (Vic) s 5.

Table 2 Existing external bodies – formal remit and powers to deal with in-scope issues

	ACCC	ACMA	ASBFEO (Small business users only)	ACSC	State and Territory Consumer Protection Bodies	eSafety	OAIC	State Small Business Commissions (For Vic, NSW, WA, SA small businesses only)	COSBOA
Payments	There are Australian Consumer Law (ACL) provisions that could be applicable to these issues, and that could be resolved user-to-user as private actions. The ACCC would not have a role in those resolutions.		Authority: May have authority if small business user has an issue that relates to a “relevant action” under section 65 of the ASBFEO Act. Power to: Facilitate discussion and refer to ADR provider.		See ACCC Some fair trading bodies may also receive reports of scams, but similarly to the ACCC do not resolve individual complaints.			Example: Victorian Small Business Commission Act 2017 Functions and powers – s 5(2): <ul style="list-style-type: none"> • (c) to receive and investigate complaints by small business regarding <u>unfair market practices or commercial dealings</u>. <ul style="list-style-type: none"> ○ To provide alternative dispute resolution between the parties involved in a complaint. • (d) to make representations to an appropriate person or body on behalf of a small business who has made a paragraph (c) complaint. • (e) to provide ADR to small businesses involved in disputes, where section 3 defines “disputes” to include a <u>contractual or commercial dispute</u> between a small business and another business, or other bodies referred to in that section. Note: section 3 defines ADR to include mediation and preliminary assistance.	
Spam	Authority: The ACCC also has power to act on behalf of consumers where there are breaches of the Competition and Consumer Act (CCA). Power: Where the ACCC believes there has been a contravention of the CCA, it can pursue formal sanctions such as infringement notices, enforceable undertakings. The ACCC cannot determine whether a breach has occurred. This must be determined by a court. This is resource intensive and the ACCC therefore only pursues this option where there is a significant systemic issue.	Authority: To respond to complaints about messages that <u>breach the Spam Act</u> and are sent to an <u>instant messaging account</u> or <u>“similar account”</u> . Power: to enforce civil penalty provisions <u>against the sender</u> through fines, injunctions, enforceable undertakings, or warnings.							
Scams	Consumers can make complaints to Scamwatch, but as outlined above, the ACCC does not respond to or act on individual complaints.			If amounts to online fraud, ACSC can refer to police for assessment. ACSC has no power to resolve.					
Fake reviews	As above, the ACCC does not resolve individual consumer complaints. However, it does have compliance and enforcement powers open to it that would assist to address the systemic underlying issues that cause these types of disputes.								
Hacking and fake accounts				If amounts to online fraud or identity theft, ACSC can refer to police for assessment. ACSC has no power to resolve.					
Content or account removal									
Ad-related issues									
Platform policies or procedures									



Australian Government

Department of Infrastructure, Transport,
Regional Development and Communications

ONLINE SAFETY, MEDIA AND PLATFORMS DIVISION / PLATFORMS AND NEWS BRANCH

Digital platforms industry external dispute resolution scheme

Feasibility study and design project final report

October 2021

October 2021 / INFRASTRUCTURE

Ownership of intellectual property rights in this publication

Unless otherwise noted, copyright (and any other intellectual property rights, if any) in this publication is owned by the Commonwealth of Australia (referred to below as the Commonwealth).

Disclaimer

The material contained in this publication is made available on the understanding that the Commonwealth is not providing professional advice, and that users exercise their own skill and care with respect to its use, and seek independent advice if necessary.

The Commonwealth makes no representations or warranties as to the contents or accuracy of the information contained in this publication. To the extent permitted by law, the Commonwealth disclaims liability to any person or organisation in respect of anything done, or omitted to be done, in reliance upon information contained in this publication.

Creative Commons licence

With the exception of (a) the Coat of Arms; (b) the Department of Infrastructure, Transport, Regional Development and Communications photos and graphics; and (c) [OTHER], copyright in this publication is licensed under a Creative Commons Attribution 4.0 Australia Licence.

Creative Commons Attribution 4.0 Australia Licence is a standard form licence agreement that allows you to copy, communicate and adapt this publication provided that you attribute the work to the Commonwealth and abide by the other licence terms.

Further information on the licence terms is available from <https://creativecommons.org/licenses/by/4.0/>

This publication should be attributed in the following way: © Commonwealth of Australia 2021

Use of the Coat of Arms

The Department of the Prime Minister and Cabinet sets the terms under which the Coat of Arms is used. Please refer to the Commonwealth Coat of Arms - Information and Guidelines publication available at <http://www.pmc.gov.au>.

Contact us

This publication is available in hard copy or PDF format. All other rights are reserved, including in relation to any departmental logos or trade marks which may exist. For enquiries regarding the licence and any use of this publication, please contact:

Director – Creative Services
Communication Branch
Department of Infrastructure, Transport, Regional Development and Communications
GPO Box 594
Canberra ACT 2601
Australia

Email: publishing@infrastructure.gov.au

Website: www.infrastructure.gov.au

Table of Contents

Executive Summary	5
Findings and Recommendations	6
Chapter 1: Introduction	7
Digital technologies have become central to how Australians conduct their daily lives and work	7
What are digital platforms?	7
Dispute resolution recommendations in the Digital Platforms Inquiry and Government response	8
EDR Scheme Feasibility Study process	8
Chapter 2: International changes since the Digital Platforms Inquiry	10
Technical and policy developments by platforms	10
International Regulatory Developments in Dispute Resolution	12
Broader policy environment and international regulatory developments	12
Chapter 3: Digital platforms' internal dispute resolution processes	13
What is issues management and what is dispute resolution?	13
Mapping digital platforms' internal dispute resolution processes	15
Chapter 4: User experiences with digital platforms' internal dispute resolution processes	19
Chapter 5: The existing external escalation ecosystem	24
Chapter 6: Government response options	28
Stakeholder responses to regulation options	30
Glossary	31

List of Figures and Tables

Figure 1. Types of digital platforms	7
Figure 2. Issues identified as in-scope for the survey	9
Figure 3. There are different types of issues, complaints and disputes	13
Figure 4. Issues management process resolution pathways	14
Figure 5. More users are satisfied with outcomes given by platforms' internal issues management processes	16
Figure 6. Platforms have greater investment in tools that suit their circumstances and business models	16
Figure 7. Platforms face challenges that result in pain points for users	18
Figure 8. Consumers and SMBs report that the current issues management landscape resolved 84 per cent of reported issues in 2020	20
Figure 9. Most consumers experienced scams while most SMBs experienced content and account issues	21
Figure 10. All platforms resolved over 70 per cent of issues reported to them internally	21
Figure 11. 48 per cent of consumers and 54 per cent of SMBs are satisfied with platforms' IDR processes	22
Figure 12. Users who received outcomes still felt that the platform could communicate better	22

Figure 13. Consumers and SMBs suffered a range of adverse consequences as a result of online issues and the dispute resolution process	23
Figure 14. Options for regulation of the digital platforms industry dispute resolution processes	29

Executive Summary

The Digital Platforms External Dispute Resolution (EDR) Scheme Feasibility Study commenced in January 2021. The purpose of the EDR Scheme Feasibility Study was to:

- review and update the evidence base that supported the Government commitment in response to recommendations 22 and 23 of the Australian Competition and Consumer Commission's (ACCC) Digital Platforms Inquiry (DPI), and
- make recommendations to Government about possible reform options, including whether to establish a Digital Platforms Ombudsman.

Recommendation 22 called for the development of minimum standards for the internal dispute resolution (IDR) systems of digital platforms. This recommendation was largely based on consultation with small businesses regarding platforms' responses to scam advertising. Feedback from stakeholders, including consumers and small businesses, suggested that improvements could be made in the IDR systems of digital platforms.

Recommendation 23 called for the Government to establish a new independent ombudsman to resolve complaints about digital platforms, or for the Telecommunications Industry Ombudsman (TIO) to take on this role if feasible.

Between January and September 2021, the Department of Infrastructure, Transport, Regional Development and Communications (Department) consulted with industry and government stakeholders, undertook research, and commissioned consumer and business surveys. Accenture was commissioned to undertake key parts of this work between March and June 2021 (**Attachment A**). The overall process mapped the current state of digital platform dispute resolution in Australia, identified shortcomings in the current internal and external dispute resolution framework and informed policy development options outlined in this paper regarding what, if any, action should be taken by government in response.

There have been significant changes since the DPI was released in 2019

Since the DPI was released in 2019, there have been significant changes in the digital industry environment, both initiated by platforms themselves with new products and processes, and by governments around the world through policy interventions. Chapter 2 provides an overview of some amendments to major platforms' internal policies that are likely to have contributed to these changes.

In terms of the regulatory environment, it has changed noticeably, with heightened global scrutiny of platforms' behaviour and increasing attempts to regulate how digital platforms deal with users and their complaints. Most notably, there have been significant developments in the European Union (EU) where legislation has been enacted or proposed to address different platform activities. The Department undertook research on international approaches to government intervention in digital platforms' dispute resolution processes. An overview of international developments is at **Attachment B**.

The digital dispute resolution ecosystem costs Australian users \$3.7 billion a year

The current digital dispute resolution landscape cost the economy an estimated \$4.2 billion in lost time in 2020, of which \$3.7 billion was borne by consumers and small businesses. This is in addition to \$188 million in direct financial losses incurred by small businesses (\$101 million) and consumers (\$87 million) - for instance, arising from scams or advertisement spending - and an unknown number of sales and opportunity losses.¹

Platforms prevent many issues, but could improve how they manage the issues that do occur

Platforms claim to have invested heavily in technology to support their issues management processes. In 2020, the Accenture report estimates that this has allowed the platforms to resolve 75 million potential issues before or immediately after they occurred. However, 4.9 million in-scope issues (see Figure 2) were still experienced by Australian users last year. Of these, half were reported to platforms, which resolved only 2 in 3 of those issues (Figure 8).

¹ Accenture Report, pages 47-49.

Only half of consumers and small businesses were satisfied with their experience of the platforms' issues management process. Users wanted more information from platforms about the process and timing, and more support and explanation of the outcomes they received. Unsatisfied users were more likely to escalate their complaint to a dispute with the platform, or escalate to an EDR body to try to find a resolution.

The existing external dispute resolution ecosystem could be improved

In 2020, 453,000 issues were reported to EDR bodies (either immediately or after the issue had gone through platforms' issues management processes), of which 2 in 3 were resolved. However, only a third of users were satisfied with the resolution they received using EDR. Feedback from consumers and small businesses suggests the EDR ecosystem is confusing for users and in many cases is unable to effectively resolve user issues, especially where the user is an individual rather than a small business.

Users are confused about where to direct their dispute, and assume that EDR bodies can resolve their problems. However, EDR bodies generally do not have powers to resolve issues and those that do have powers can only consider systemic issues rather than individual cases.

Research and analysis of the formal powers of existing EDR bodies in Chapter 5 leads to three key observations:

1. Small businesses have resolution pathways for some issues, but it is unclear which is the most effective.
2. Individuals do not have satisfactory resolution pathways for most in-scope issues.
3. The ACCC and State and Territory consumer protection bodies could make more use of their powers to address the underlying causes of in-scope issues.

Some shortcomings in the current system are due to under resourcing; lack of public information about available services; platforms and EDR bodies lacking formal communication pathways, so that platforms are unresponsive when EDR bodies reach out; and EDR bodies lacking or not utilising their full range of powers to help users.

s47C - deliberative processes

Chapter 1: Introduction

Chapter Overview

This chapter introduces the digital platforms market, and gives background leading to the EDR Feasibility Study.

Digital technologies have become central to how Australians conduct their daily lives and work

Australia's technology sector, which includes digital platforms, is a critical pillar of the economy. Digital activity currently contributes \$426 billion to the Australian economy and generates \$1 trillion in gross economic output.²

In Australia and other jurisdictions, there are questions about the role and impact of digital platforms, stretching from alleged anti-competitive conduct, the amount and security of user information collected by platforms, and concerns over the prevalence of disinformation and other harmful content.

Lack of competition in the digital industry can undermine the benefits able to be realised by users. In particular, Google and Facebook both have huge market shares and in many cases are critical and unavoidable partners for Australian businesses. Google has a monthly audience of 19 million and Facebook of 17 million in Australia. Google has a substantial market power in general search services, holding a market share of between 93-95 per cent since 2009, while over 80 per cent of the time users spend on social media services is on Facebook's platforms.³

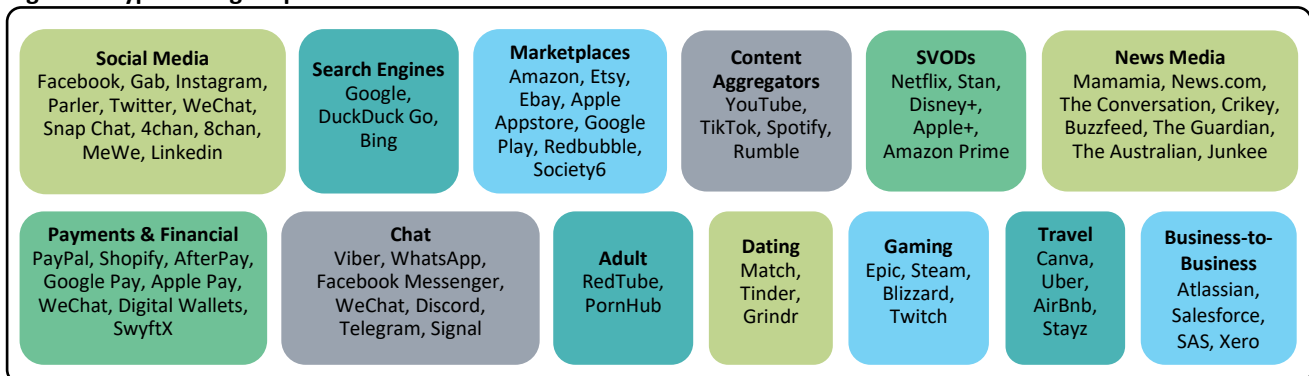
It is important to consider the relative power of platforms and users in dispute resolution. Users are reliant on platforms to conduct their lives, and in most cases have no other alternative provider through which to access the same services.

What are digital platforms?

'Digital platforms' is an umbrella term that covers a diverse range of companies. They can be described as businesses that offer services or utilities to users via an online interface. They generally require users to establish profiles to access them - which usually gives the user a more personalised service, and allows the platform to collect data on that user and/or a subscription fee. Users may be all one type, or have different types depending on the service (e.g. sellers and buyers, administrators, affiliates, etc). Platforms can also be described by their business model - subscription or free services that make money through targeted online advertising services and/or micro transactions and fees.

The diagram below shows examples of major businesses in existing service categories. However, new and smaller platforms also fall within those categories. Services outside of these categories are also continually emerging.

Figure 1. Types of digital platforms



² AustCyber Australia Digital Trust Report 2020.

³ ACCC, DPSI September 2020 Interim Report, B7.

Dispute resolution recommendations in the Digital Platforms Inquiry and Government response

In the DPI, the ACCC made two recommendations relevant to dispute resolution. First, it found that the internal dispute resolution (IDR) processes of digital platforms were not working for consumers and businesses and needed to improve. To do this, it recommended that the Australian Communications and Media Authority (ACMA) develop minimum IDR standards for digital platforms (Recommendation 22), which would set out specific requirements, including transparency, visibility, accountability, and data safety, among others.

ACCC also recommended that Government establish an independent ombudsman to resolve complaints about digital platforms (Recommendation 23), or that the Telecommunications Industry Ombudsman (TIO) could take on this role if it were feasible to do so.

The Government committed to a pilot EDR Scheme

The Government Response and Implementation Roadmap for the Digital Platforms Inquiry,⁴ committed to develop a pilot EDR scheme in 2020, to inform its decision on whether to establish a Digital Platforms Ombudsman. The Government acknowledged an EDR mechanism would need to be tightly integrated with existing IDR processes and that there was merit in requiring digital platforms' IDR processes to be clear and transparent, and that they are the preferred resolution pathways before EDR mechanisms. The Government committed to consider the outcomes of the pilot and make a decision on an ombudsman in 2021.

The Department undertook a feasibility study to develop advice to Government

The EDR Scheme Feasibility Study ran from January to September 2021. This allowed the significant changes in the digital industry environment and both international and domestic regulatory developments to be considered (as discussed in the following chapter). It included research on international legislation, user experiences with IDR and EDR processes, and the digital platforms' dispute resolution landscape. This research informed the analysis and conclusions in this report, and the possible options available to Government to improve the current system in Chapter 6.

EDR Scheme Feasibility Study process

The feasibility study took a first principles approach

The study examined several foundational questions:

- What has changed since 2019, and have any of these changes resolved the issues identified in the DPI? (Chapter 2)
- What do digital platforms' existing IDR processes look like, and are there any gaps? (Chapter 3)
- Are there consumer and small business disputes that are going unaddressed by digital platforms' IDR processes? And if so, what are the costs of those disputes going unaddressed? (Chapter 4)
- Are there effective EDR mechanisms to support consumers and businesses deal with unresolved disputes? (Chapter 5)
- **s47C - deliberative processes**

To answer these questions, the department conducted or commissioned several research projects:

- An examination of international regulatory developments relating to digital platforms' complaint handling processes;
- Mapping of digital platforms' issues management (including IDR) processes;
- Survey of consumer and small to medium business (SMB) issues reported to and about digital platforms;
- Research on existing dispute resolution bodies, their powers and governance structures.

⁴ [Government Response and Implementation Roadmap for the Digital Platforms Inquiry \(treasury.gov.au\)](https://www.treasury.gov.au/government-response-and-implementation-roadmap-for-the-digital-platforms-inquiry)

The Department's research focused on the major platforms, and issues that are unaddressed by either existing or developing legislation

The Department contracted Accenture to conduct the IDR mapping and surveys, as detailed in Chapters 3 and 4. Accenture's research focused on the major platforms operating in Australia, including Facebook, Google, Twitter and eBay. For the surveys, its research also defined in-scope complaints as the following:

Figure 2. Issues identified as in-scope for the survey

Categories of in-scope issues	Description
Ad-related issues	Issues around ads such as being incorrectly billed for an ad, ad not delivering promised or expected results, transparency around ad effectiveness and unexpected changes to platform algorithms that reduce ad visibility.
Content or account removal	When a platform suspends or removes an account or content posted by a user. For businesses this can result in loss of followers or customer data on the platform.
Fake reviews	Fake reviews or comments e.g. fake reviews on a business page to boost sales, or fake, vexatious complaints received from unsatisfied customers.
Hacking and fake accounts	Account hacking or fake accounts created to mimic another user, or fake accounts created to engage in offensive or inauthentic behaviour.
Payments	Payment and transaction issues between users, on a platform that has a payment system or functions as a marketplace.
Platform policies and procedures	Issues that users have with the platform's complaint handling policies and processes. Examples include where users couldn't find information on how to make a complaint or contact the platform, and where users were told they were in breach of platform guidelines but didn't know which one.
Scams	Content that is false and designed to trick users into spending money, share their personal information etc. Includes online shopping, investment, dating scams, fake ads and phishing.
Spam	Content that is unsolicited, annoying and usually posted or sent in bulk to users.

Accenture excluded complaints dealing with offensive content, prohibited or regulated content, public misinformation, and infringements (for example, intellectual property and privacy complaints). Although complaints by consumers and businesses on these issues are important, we have chosen not to focus on them in this report as they are largely addressed under existing legislation or industry codes, some of which have been introduced following the release of the DPI report. Other issues, such as password resets, are too minor to attract a regulatory role for Government.

The Department consulted with industry and across government

To support the feasibility study, the Department convened an Advisory Panel to consult with other government agencies and key industry stakeholders. A summary of the stakeholder feedback and consultation outcomes are in **Attachment C**.

The role of the panel was to provide more information and data for consideration, discuss the research and outcomes of the study, and give feedback on options for a possible EDR Scheme. Industry members were invited to select meetings to provide industry perspective as needed. The panel did not have a decision-making role in the study or scheme.

Chapter 2: International changes since the Digital Platforms Inquiry

Chapter Overview

As noted by the ACCC in its September 2020 Digital Platforms Services Inquiry report (page G1), ‘there has been a broad international trend of governments and regulators focusing on the role and practices of digital platforms. At the same time, platforms have themselves announced a range of self-regulatory measures seeking to address identified issues.’ This chapter examines the developments that have arisen since the ACCC’s DPI Final Report in 2019.

Technical and policy developments by platforms

Platforms continuously develop and expand their services offerings, as well as the mechanisms they use to address harms and issues on their platforms. Outlined below are some examples of how platforms have developed since 2019. Chapter 3 (IDR mapping) further outlines some of the prevention mechanisms that platforms have invested in.

Facebook⁵

In February 2020, Facebook released a White Paper on online content regulation.⁶ The Paper calls for new regulatory frameworks for online content so that platforms make decisions that minimise harm while respecting freedom of expression.

The White Paper touches on dispute resolution:

Regulation could also incentivise—or where appropriate, require—additional measures such as ...a channel for users to appeal a company’s removal (or non-removal) decision on a specific piece of content to some higher authority within the company or some source of authority outside the company.⁷

The above quote is likely to be a reference to the recently established Oversight Board, whose creation was planned since November 2018. The Oversight Board, outlined below, functions like a court and reviews Facebook’s enforcement decisions. It is the most notable development in dispute resolution since 2019 relevant to Facebook.

Other developments

Facebook invested \$US130m in its independent Oversight Board to hear appeals from users about content concerns, after internal appeals have been exhausted. On 15 July 2021, Facebook released its First Quarterly Update⁸ on the Oversight Board, in which it committed to implement, fully or in part, 14 of the Board’s 18 non-binding recommendations – including giving users more specifics about why and how flagged content violates a policy, flagging when content is removed by automated systems rather than human reviewers, and introducing a new online Transparency Centre to educate users about its rules and how they are applied by Facebook.

Facebook’s Q1 2021 Transparency Report illustrates an upward trend in proactive action under most of its policies, due in part to improvements in Artificial Intelligence and machine learning technologies. For example, 8.8 million pieces of

⁵ Facebook changed its company name to Meta on 1 November 2021. Meta includes in its portfolio Facebook app, Messenger, Instagram, WhatsApp, Oculus, Workplace, Portal and Novi.

⁶ [Charting A Way Forward: Online Content Regulation White Paper](#)

⁷ [Charting A Way Forward: Online Content Regulation White Paper](#), p 10.

⁸ [Facebook Q1 2021 Quarterly Update on the Oversight Board](#)

bullying and harassment content was actioned in Q1 2021, compared to 6.3 million in Q4 2020. Despite this, the Report notes:

[Machine learning] technology is very promising but is still years away from being effective for all kinds of violations. For example, there are still limitations in the ability to understand context and nuance, especially for text-based content. This creates additional challenges for proactively detecting certain violations.⁹

Additionally, consistent with the recommendations of the Oversight Board, Facebook launched a Transparency Center in May 2021 to provide a hub for integrity and transparency work. It has published an Integrity Timeline,¹⁰ highlighting key events and policy updates that improve the integrity and transparency of the platform.

s47G - business information

s47G - business information

s47G - business information

International Regulatory Developments in Dispute Resolution

Since 2019, the landscape of dispute resolution around the world has shifted. We are seeing increased global scrutiny of platforms' behaviour, and attempts to govern how digital platforms deal with users and their complaints. Detailed explanations and analysis of major international shifts are provided in **Attachment B**. Most notably, there have been significant developments in the European Union (EU) where legislation has been enacted or proposed to address different platform activities, including:

- **Regulation on Platform-to-Business Trading Practices** (*Effective July 2020*): Applies to platforms through which business users offer goods or services to consumers (Amazon market place, eBay, Uber, Facebook Marketplace, app stores, price comparison websites). Requires platforms to meet minimum standards for internal complaint-handling systems and terms and conditions, and a commitment to engage in good faith with named mediators. Also requires platforms to give statements of reasons for decisions to restrict, suspend or terminate use of their services.
- **Digital Services Act** (*Proposed December 2020*): Applies to "online intermediary services" on a tiered basis, with higher obligations for services that have a larger reach and presence in the EU. Requirements include minimum standards for terms and conditions, internal complaint-handling systems, and that providers engage with certified out-of-court dispute settlement bodies on decisions.

Broader policy environment and international regulatory developments

Trust in platforms is at a low – globally, trust in the technology sector has fallen 10% since 2019.¹⁷ This has been accompanied by growing sentiment around the world (from the public and governments) that more should be done to address the negative impacts of digital platforms in society.

*If public opinion continues to trend in negative directions for the technology sector, both in the United States and around the world, it likely will broaden support for government actions that regulate technology...*¹⁸

Some examples of international regulatory or policy developments evidencing this sentiment towards digital platforms, though not necessarily in relation to their dispute resolution processes, are as follows.

- The United Kingdom (UK) has proposed a new pro-competition regime for digital markets, which will involve designating digital platforms with 'strategic market status', codes of conduct for those platforms, and implementation of pro-competition interventions.
- The United States of America (USA) has taken action designed to improve competition in the digital platform market, including antitrust suits brought by the Federal Trade Commission. In addition, President Biden has signed an executive order that involves initiatives to tackle competition issues such as "Big Tech" purchasing competitors, gathering personal information on users, and unfairly competing with small businesses.
- Similar themes can be seen in the five bills introduced in the US House of Representatives in June 2021, designed to improve interoperability and data portability; prevent "killer" acquisitions; prevent self-preferencing a platform's own products over a competitor's; updating merger requirements; and preventing other discriminatory conduct.¹⁹

¹⁷ [2021 Edelman Trust Barometer](#).

¹⁸ [West, D. \(2021\) Techlash continues to batter technology sector. \(Brookings.edu\)](#)

¹⁹ [Congress unveils 5 bipartisan bills that mark its biggest step yet in regulating tech giants like Amazon, Google, Facebook, and Apple \(businessinsider.com.au\)](#)

Chapter 3: Digital platforms' internal dispute resolution processes

Chapter Overview

Like any business, digital platforms have issues management processes to identify, minimise and resolve issues that occur on their services. However, when digital platforms cannot or do not resolve issues they may escalate into disputes. Disputes can be actioned through both platforms' internal dispute resolution processes and third party external dispute resolution processes. This chapter focuses on those internal dispute resolution processes.

What is issues management and what is dispute resolution?

*Problems arise every day between businesses, their customers, suppliers and employees. Most of them are dealt with quickly and efficiently through common sense, but sometimes they turn into disputes which needs further understanding to resolve.*²⁰

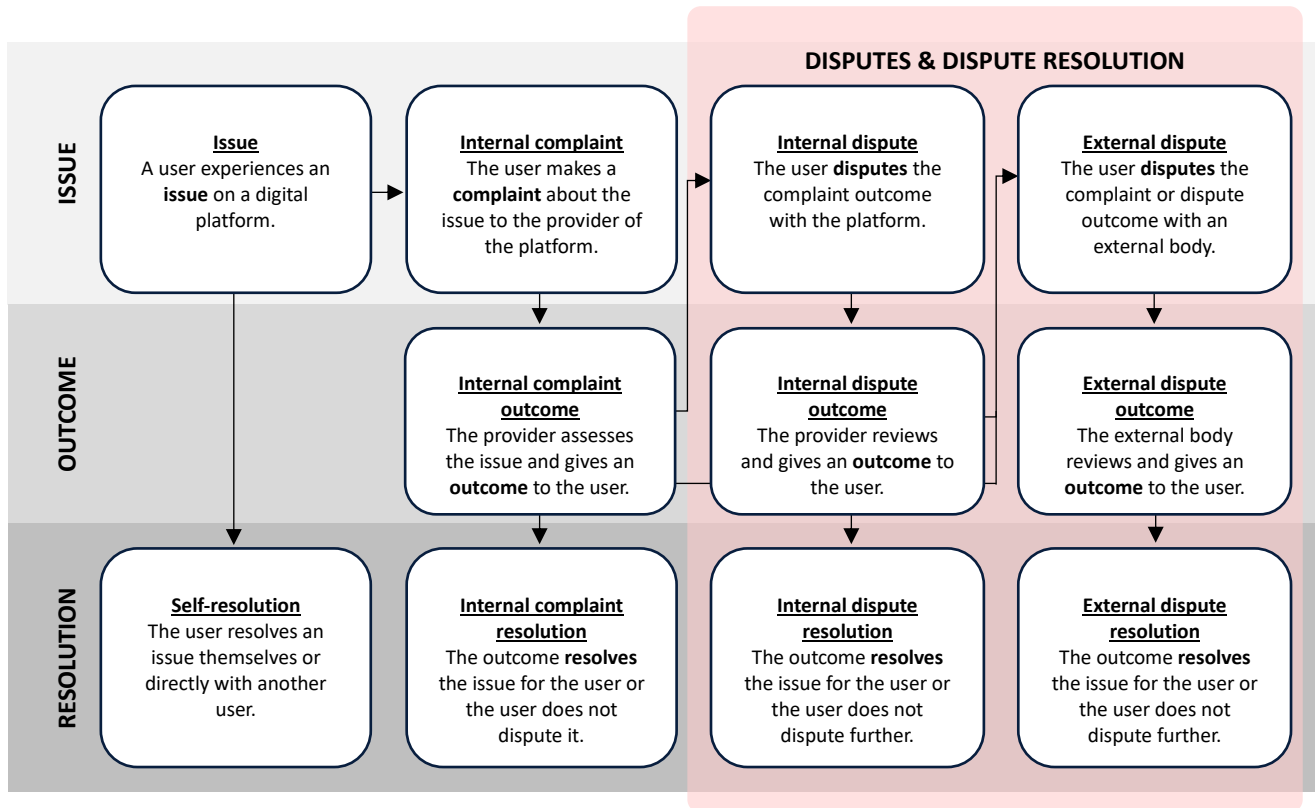
In its research, Accenture identified that digital platform users travel through a number of phases of issues management, and that resolution can happen at multiple points in that journey. Figure 3 outlines the terminology used throughout this report, and Figure 4 illustrates the various resolution pathways available to users.

Figure 3. There are different types of issues, complaints and disputes

Category	Definition
Issue	An issue is a negative experience or content encountered on a platform by a user. Issues include both un-actioned and actioned issues. See Figure 2 for a list of in-scope issues.
Un-actioned issue	An un-actioned issue is when an issue is observed or experienced on a platform by a user, but the user takes no action to resolve it.
Actioned issue	An actioned issue is when an issue is observed or experienced on a platform by a user, who then takes action to resolve it through self-resolution or a complaints handling process.
Internal complaint	An internal complaint is when a user first contacts the platform to resolve an issue.
Internal dispute	An internal dispute is when a user disagrees with the decision of a platform, after the platform assesses their complaint, and follows up with the platform to seek a different outcome.
External dispute	An external dispute is when a user contacts an external body (such as reporting the issue to ACCC, fair trading bodies, or ombudsmen) about an internal complaint or internal dispute with a platform.
External complaint	An external complaint is when a user contacts an external body about the issue without first going through a platform's complaint or dispute process.
Resolved	An issue is resolved if the user reports it as resolved, whether to their satisfaction or not.
Unresolved	An issue is unresolved if the user reports that no resolution has been reached, such as when the issue is ongoing without a resolution in sight, there were too many roadblocks for the user to progress the issue, or the platform or third party do not engage further with the user. There are cases where the platform may have deemed an issue resolved and the user disagrees with this decision, which can result in dispute.

²⁰ [Five steps to resolve your dispute | Australian Small Business and Family Enterprise Ombudsman \(asbfeo.gov.au\)](#)

Figure 4. Issues management process resolution pathways



Good issues management practices and good dispute resolution processes go hand in hand

Issues management should aim to prevent and address issues before they escalate. Platforms can do this by having:

- Clear guides and policies that set up expectations for the use of a service, the outcomes a user can expect if they report an issue, and both parties' rights and responsibilities;
- Strategies to understand how and why issues occur, and to build insights into the issues management process;
- Reporting systems that are both easy to find and easy to use;
- Processes to obtain feedback from users, and to review guides and policies that aren't clear or exacerbate issues.

Supporting the accountability of essential industries

Where an industry fails to resolve issues regularly experienced by their customers, and those issues are of sufficient impact to warrant intervention, there may be a role for Government to ensure there are avenues available to those customers to seek resolution. If customers are experiencing reoccurring issues, or a business is unable or unwilling to solve a customer's legitimate problem, external bodies provide a mechanism through which a dispute can be escalated and resolved.

In many sectors, the Government has established frameworks requiring industry to act in a fair, transparent and accountable way. This may be through standards setting out how companies should act to achieve a base level of fairness, transparency and accountability in their interactions with customers. It may also include ombudsmen or regulators to mediate or hold businesses accountable for solving the issues experienced by their customers.

Mapping digital platforms' internal dispute resolution processes

In its response to the DPI, the Government said that digital platforms operating in the Australian market should have IDR processes that provide a clear, transparent avenue for people to raise concerns with service providers before needing to escalate concerns to an external body.²¹

In order to understand whether platforms already have effective IDR processes in place, Accenture mapped the issues management systems (including IDR processes) of four major digital platforms in Australia (Google, Facebook, Twitter and eBay)²² and highlighted common strengths and weaknesses. Mapping these four major platforms allowed for representation from social media, search engines and marketplace platforms, each of which involves different types of user-to-user interactions.

Platforms favour automated over manual approaches to issues management

Over time, digital platforms' issues management systems have faced challenges from increasing and high user numbers; rapidly evolving, complex and emerging issues; and a growing number of 'bad-actors' attempting to cause harm to other users. Digital platforms have responded to these challenges by employing automated approaches using new technologies designed to anticipate or quickly address the majority of issues. Platforms also employ self-service mechanisms, which rely on users to work through a series of steps to resolve their own problem before they are able to make a complaint to the platform.

This 'automated' approach is generally effective and highly efficient to respond to most issues and requires little or no staff resources. Accenture estimates that by relying more on automated issues management, platforms save approximately \$4.8 billion per annum (at a cost of \$4.2 billion, compared to a cost of \$9 billion per annum if they only used manual processes). Accenture's report found that digital platforms increase user satisfaction if their issues management systems are faster and easier to use.

However, the efficiency of automated systems can come at the expense of flexibility, transparency and communication. Additionally, an automated approach often doesn't account for emerging or complex issues, or differences in tone and cultural meaning, so can fail some users altogether. The result is that it is very difficult for users to access in-person case management for complicated issues, and that these issues are therefore more likely to become disputes.

Automation can prevent potential issues before users experience them

Platforms' technology-based interventions are primarily targeted at issues prevention, and include machine learning, artificial intelligence programs, and analytical algorithms, supported by specialist review teams.

Platforms report that in 2020 their issues prevention methods stopped 9.3 billion false and misleading ads and spam, 5.8 billion policy violating social media accounts, 99 million false and misleading COVID-19 claims and ads, and 55 million fake reviews globally. For content not captured by initial screening, platforms employ those same technologies to proactively remove 'potential problems' before users experienced them.²³ In 2020, platforms report that 75 million (95 per cent) potential problems were removed from Australian platforms using issues prevention technologies.²⁴

When users do encounter issues, they are first encouraged towards self-resolution

Users who experience issues travel through escalating stages of a platforms' issues management process. According to Accenture's consumer and small business surveys (see Chapter 4), approximately 4.9 million in-scope issues are experienced by Australians each year, of which users will attempt to resolve 4.2 million. Of this, 2.4 million actioned

²¹ [Government Response and Implementation Roadmap for the Digital Platforms Inquiry \(treasury.gov.au\)](#)

²² Google and Facebook alone own the top 5 social media platforms in Australia - 78 per cent of Australian internet users aged 16 to 64 used both YouTube (owned by Google) and Facebook in 2021, while 65 per cent used Facebook Messenger, 55 per cent used Instagram and 39 per cent used WhatsApp, all owned by Facebook. The 6th most-used platform in Australia was Twitter, at 30 per cent. We are social/Hootsuite, [Digital 2021 – Australia report](#)

²³ Accenture Report, p 18; Global figures provided by digital platforms and transparency reports.

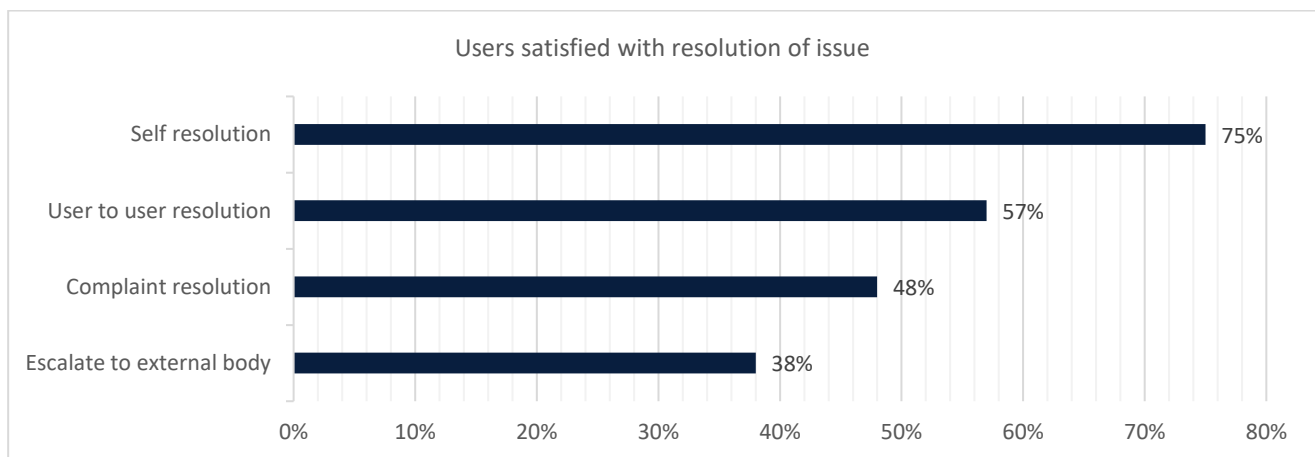
²⁴ Accenture Report, pp 27-28; Global figures provided by digital platforms and transparency reports.

issues are escalated to platforms' internal complaints or dispute processes, and 1.6 million are resolved by the user, using either the platforms' user-driven tools or directly with other users.

All major platforms follow a similar process of user-driven tools followed by platform-driven tools.²⁵ Platforms have 'gateways' that encourage self-resolution, so that minor issues are given timely and convenient outcomes without the user needing to report a complaint. This allows platforms to give greater attention to more complex issues, which more often require human-led methods to resolve.

Users also report greater satisfaction with outcomes made earlier in the issues management process (Figure 5). 75 per cent of users were satisfied with the outcome when using self-resolution tools, compared to only 38 per cent of users who sought an outcome from an external body after going through IDR. This is not surprising as issues that are resolved immediately by automated means are more likely to be simple issues, whereas those that are escalated to an external body not only take the user more time, they are more likely to involve complex issues and disagreements between parties about the appropriate solution.

Figure 5. More users are satisfied with outcomes given by platforms' internal issues management processes



Platforms apply different issues management tools depending on their business model

While all platforms use a common baseline of user-driven and platform-driven tools that are both automated and manual, each has a unique service offering and has therefore focused additional resources on tools that support their particular business model. [s47G - business information](#)

Platforms will sometimes prioritise users with which they have a financial transaction, such as businesses that pay for advertising or premium products. This can mean that such users receive additional or better customer support tools and account managers to assist them with issues.

Figure 6. Platforms have greater investment in tools that suit their circumstances and business models

	Google	Facebook	eBay	Twitter
AI scanning / removal of content		✓	✓	✓
AI complaint review	✓	✓		
Human complaint review	✓	✓		

²⁵ Examples of user-driven tools include self-help centres, user-to-user resolutions, and real-time reporting (where a user engages with a tool that helps them remove content from their feed immediately). Examples of platform-driven tools include complaints centres, and dedicated teams and AI doing content screening.

	Google	Facebook	eBay	Twitter
Dedicated customer service teams				✓
Product-specific mechanisms	✓	✓		
Self-service / self-help	✓	✓		
Dedicated complaints portal	✓		✓	✓
Complaint tracking			✓	✓
Proactive outcome communication			✓	✓
Regulator portal for reporting / removing regulated content			✓	
Independent dispute review body		✓		
'Strike' systems for offending users	✓			✓

All platforms' issues management processes are underpinned by Terms of Use

All major platforms have Terms of Use (ToU) (also known as Terms of Service or Terms and Conditions) that let users know what interactions are and are not allowed on the platform; the user's and provider's rights, responsibilities, and obligations to each other; and how breaches of ToU may be handled. While platforms may have different combinations of tools and processes for issues resolution, ToU are common practice for industry.

ToU can often use legal language, so platforms sometimes have plain language policy centres, such as Facebook's Community Standards or Help Centre, to better communicate their rules to users. Some platforms will direct users to those policies in an outcome, especially when the platform has used AI to review and make a decision, as a means of explaining their decision. However, this can sometimes add to a user's confusion if they disagree with that policy or decision, or if it's not clear what part of the ToU has been breached.

Some of the platforms consulted in this study suggested that giving users too much information about how a particular policy is applied would lead to 'gaming of the system', allowing bad actors to circumvent the platform's policies for example by using proxy language that won't be picked up by automated detection technology. Other platforms prefer to explain the reasons for their decisions and actions in more detail, to avoid misunderstanding and further complaints.

The risk of gaming must be balanced against user needs for transparency and consistency. The data suggests that a lack of transparency leads to frustration among users, further disputes, and makes it difficult to hold platforms accountable for consistently enforcing their own rules.

Platforms face challenges that lead to pain points for users

If they do make a complaint, most users expect a more tailored issues management experience than what they receive. Platforms are moving away from personalised outcomes and information. As a result, issues that do lead to disputes are more complex, such as account hacks or scams, and have a more profound impact on users and SMBs.

Users are more likely to experience pain points than SMBs, perhaps reflecting the different transactional relationships platforms have with each type of user (see Figure 7). The top pain points for users were that the platform did not direct them to other resources, followed by the platform not providing enough information or feedback. In both cases, there is a need for information and transparency to help users resolve the issue and prevent it from happening in the future.

Figure 7. Platforms face challenges that result in pain points for users

Challenges faced by platforms	Resulting pain point for users
Handling the immense scale and scope of issues has led to the design of highly automated, scalable solutions	<ul style="list-style-type: none"> Complex cases don't receive tailored solutions Users are not always given the opportunity to speak with someone Users expect the significant amount of personal data available to platforms to be used to help resolve issues quickly, rather than having to tell their story or prove their identity at multiple stages.
Addressing a mix of complaints that differ in their complexity and severity makes it difficult to provide standardised approaches and resolution timelines	<ul style="list-style-type: none"> Limited clarity on resolution timelines Users are unaware of whether their complaint has been actioned Complaints that are important to users but low priority for platforms have extended resolution times (weeks or months) Users are far more satisfied and confident that action is being taken when they understand the process Consumers expect rapid responses and don't tolerate unexplained delays
Transparency of process, rules and decisions can lead to gaming the system and increase risk	<ul style="list-style-type: none"> Decisions and actions taken by platforms are unclear and confusing. Users want to understand the reasons behind decisions, not just which rules they are said to have broken. Users seek 'workarounds' to resolve an issue, sometimes via informal community groups or advice forums.
Marketplaces need to balance consumer and seller interests	<ul style="list-style-type: none"> Sellers may perceive a decision as biased in favour of the consumer and vice versa
Fake reviews can be subjective in nature and difficult for platforms to determine if they are fake	<ul style="list-style-type: none"> SMBs find it difficult to remove fake reviews Fake reviews can remain 'live' for days and weeks before removed (while platform investigates)
Breadth of issues and platform products means no single EDR body in Australia ('one stop shop') for platforms to refer users for escalation	<ul style="list-style-type: none"> Platforms are unclear or do not communicate EDR options Users are confused about where to go next and how to resolve

Platforms must continue to invest in their issues management processes

The pain points above illustrate that more can be done to improve user outcomes and experiences, as well as to reduce the cost of dispute resolution processes for users, SMBs and EDR bodies.

s47C - deliberative processes

Chapter 4: User experiences with digital platforms' internal dispute resolution processes

Chapter Overview

In the DPI Final Report, the ACCC found that Australian consumers and small to medium businesses (SMBs) have had negative experiences with the IDR processes of major digital platforms. This chapter examines the experiences of Australians users who have gone through platforms' IDR processes.

The Department engaged Accenture to survey Australians, to better understand the size and scope of Australians' issues with digital platforms' IDR processes. A summary of Accenture's survey results is outlined in this chapter, with the full report at **Attachment A**.

Accenture conducted two surveys – one each for consumers and SMBs – focusing on the in-scope issues in Figure 2. Accenture surveyed 8,334 consumers aged over 18 and 1,471 SMBs, of which 2,988 consumers (36 per cent) and 500 SMBs (33.9 per cent) reported experiencing an in-scope issue on a digital platform within the last 5 years. Accenture used these samples to calculate prevalence in the Australian population. Accenture estimates that 1 in 5 Australian consumers and 1 in 3 SMBs experienced an in-scope issue on a digital platform in 2020 and took action to try to resolve it. Issues, complaints and disputes are separate stages in a user's issues management journey, and are defined by which channels a user went through to communicate their problem and how they escalated their issue. See Figure 3 for definitions.

2 in 3 issues that are reported to platforms are resolved by platforms

Accenture identified that Australian users (consumers and SMBs) experienced 4.9 million²⁶ in-scope issues on digital platforms in 2020, as demonstrated in Figure 8. Of this:

- 1.6 million were resolved by the user through user-led resolution tools.
- 2.4 million were reported to digital platforms, which then resolved 1.6 million (66 per cent) of the issues reported to them.
- Of the issues unresolved by platforms, 304,000 were escalated to an external body, which then resolved a further 217,000 (9 per cent of issues reported to platforms).
- 25 per cent of the issues reported to platforms were unresolved by either platforms or an external body.²⁷

Most actioned issues were experienced on social media, in particular, on Facebook

The majority of actioned issues were experienced on social media (64 per cent of consumer issues, and 65 per cent of SMB issues), followed by marketplaces (23 per cent and 13 per cent respectively), and search engines (6 per cent and 18 per cent respectively). Specifically, consumers said that the majority of actioned issues were experienced on Facebook (46 per cent) and eBay (17 per cent), while SMBs said that the majority of actioned issues were experienced on Facebook (38 per cent) and Google (18 per cent).

Consumers were much more likely to report scams (28 per cent), of which the majority were fake ads (31 per cent). SMBs experienced issues with content and account removal (20 per cent) and ad-related issues (16 per cent). Both consumers and SMBs also reported a high number of issues with hacked and fake accounts (24 per cent and 16 per cent respectively). See Figure 9.

²⁶ This total is found by taking the number of respondents with in-scope issues in 2020, divided by the number of survey starters, to get an estimate percentage of total population or small businesses with an in-scope issue in 2020. That number is then multiplied by the number of Australians over 18 or the number of small businesses in Australia (whichever is relevant). The total was then validated against third party sources, such as Scamwatch data and complaints to the TIO, and with the digital platforms, to make sure they're generally consistent.

²⁷ This number includes 354,000 unresolved internal complaints, 173,000 unresolved internal disputes and 88,000 unresolved external disputes.

Figure 8. Consumers and SMBs report that the current issues management landscape resolved 84 per cent of reported issues in 2020

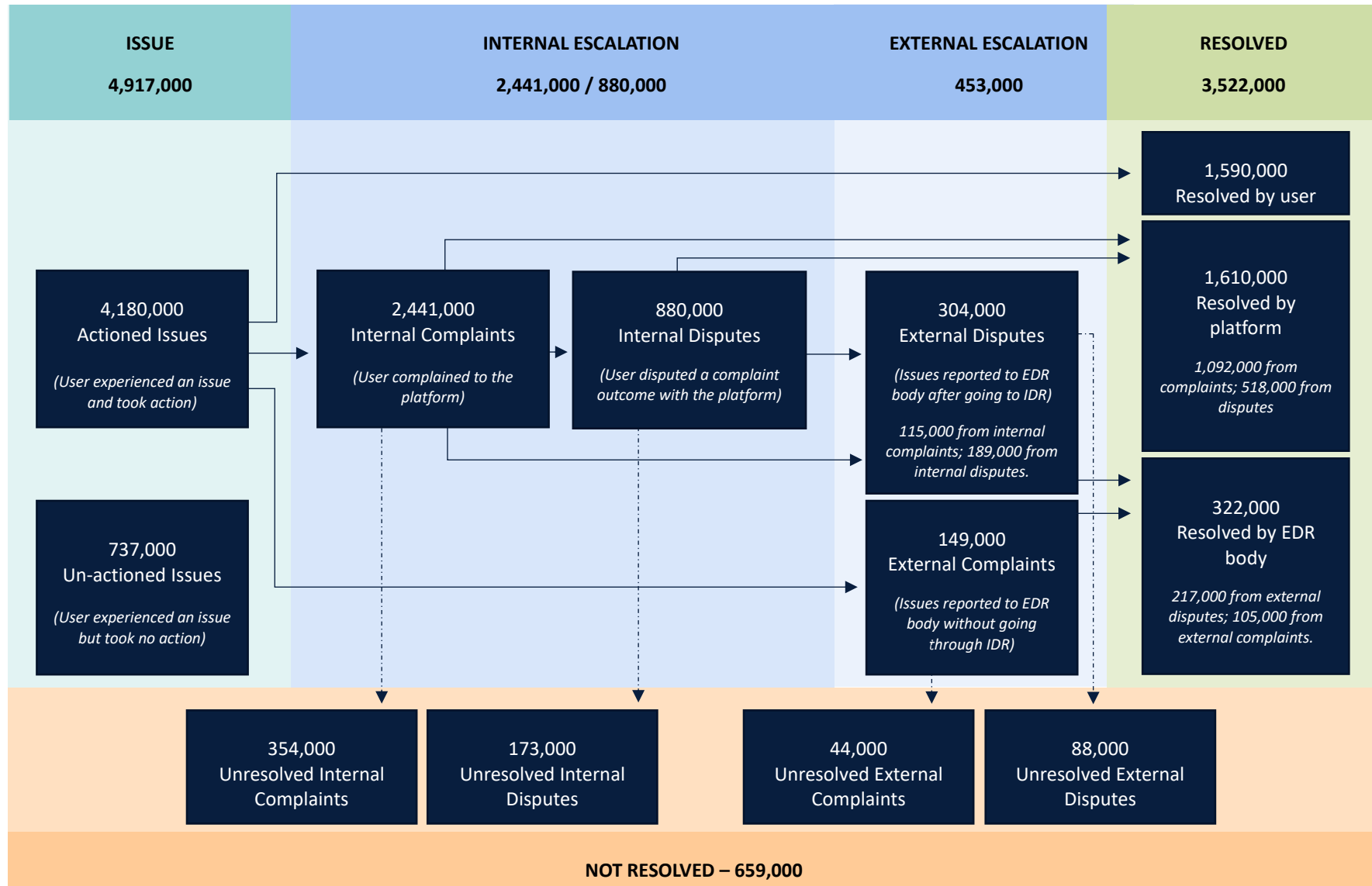
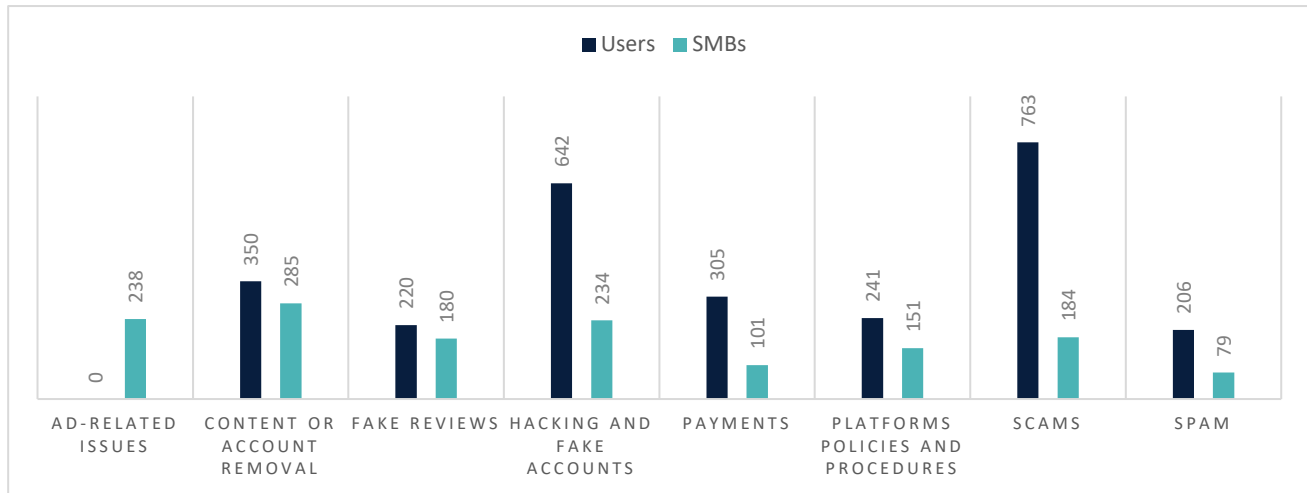
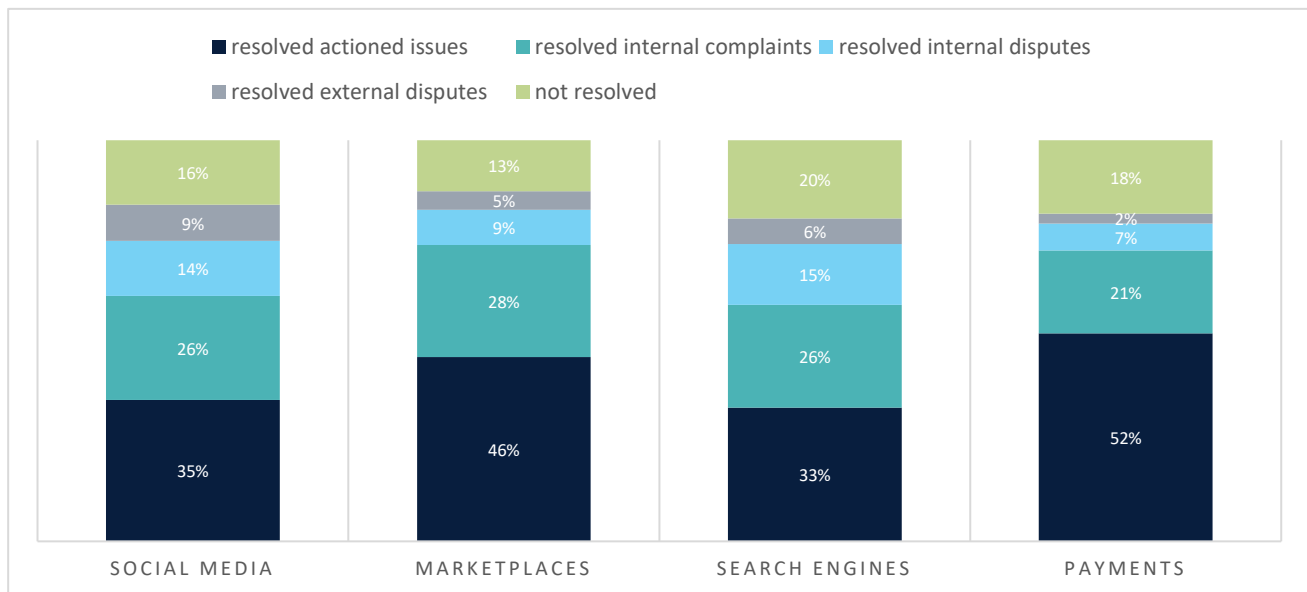


Figure 9. Most consumers experienced scams while most SMBs experienced content and account issues

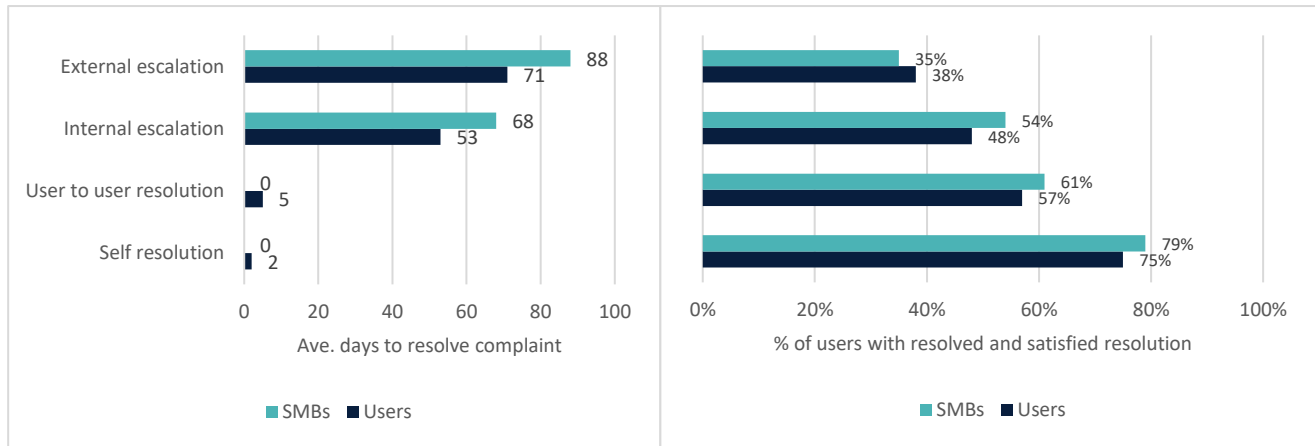
While users experienced more issues on social media platforms, all platforms had similar resolution rates for their IDR processes. Social media resolved the lowest number of issues internally (75 per cent), while marketplaces resolved the highest number (83 per cent). See Figure 10.

Figure 10. All platforms resolved over 70 per cent of issues reported to them internally

Platforms can improve user outcomes by improving their user-led and IDR processes

Users reported that when platforms offered self-resolution (such as flagging and reporting functions and help centres) and user-to-user resolution options (such as forums), those options were at least 10 times faster and more satisfactory to consumers and SMBs than IDR options. However, for those consumers and SMBs that had to use a platforms' IDR process, only about half were satisfied with the outcome they received (Figure 11). This demonstrates that, while platforms should be encouraged to increase their user-led resolution options, they also need to make improvements to their IDR processes to provide additional support in cases where user-led resolution is not sufficient.

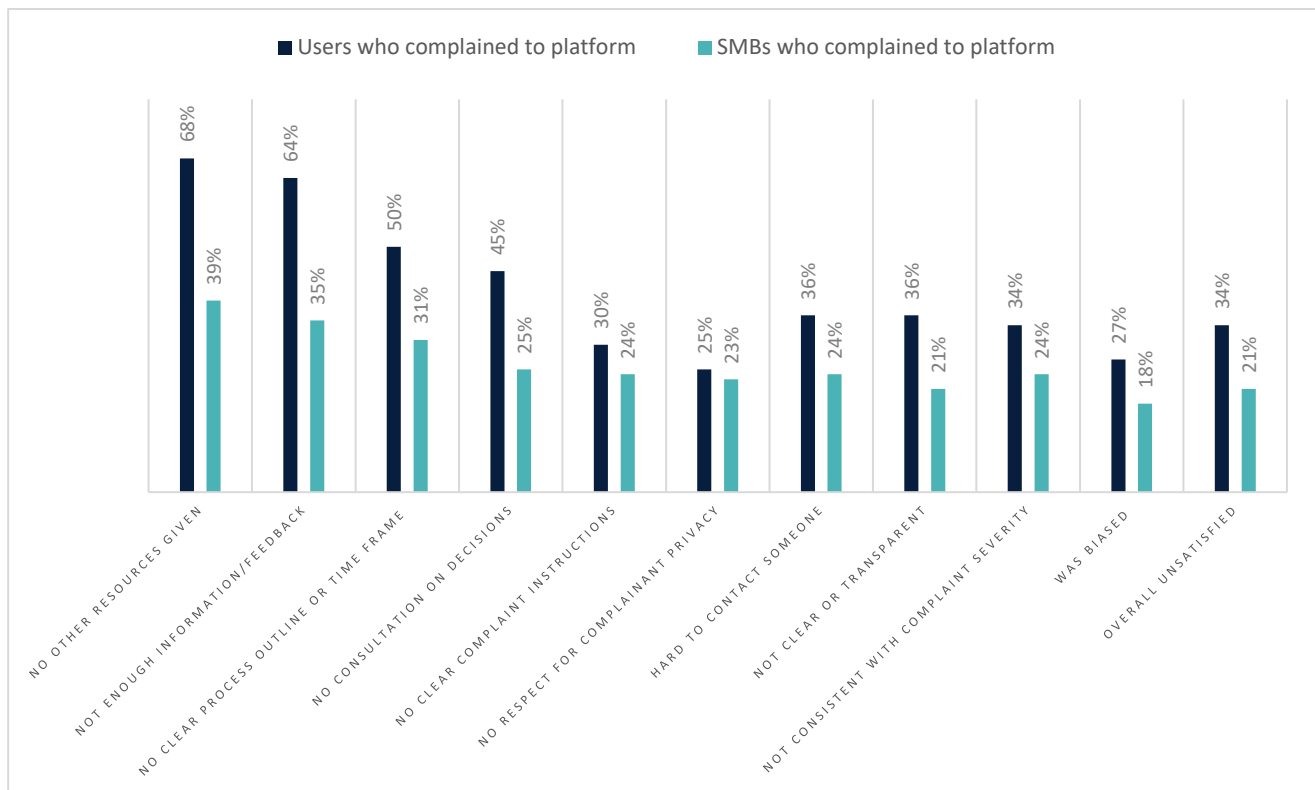
Similarly, when a user went to an EDR body, the process was even longer and less satisfying. However, this is often because the issues escalated to third parties can be the most complicated to resolve, and because the EDR body needs to work with the platform for a resolution.

Figure 11. Only 48 per cent of consumers and 54 per cent of SMBs are satisfied with platforms' IDR processes

Businesses were more satisfied with the IDR processes of digital platforms than individuals

In its surveys, Accenture asked users who went through IDR processes to identify where they thought IDR processes most need improvements. 64 per cent of consumers and 39 per cent of SMBs thought the platform did not provide enough information or feedback during the IDR process, and 68 per cent of consumers and 35 per cent of SMBs thought that the platform didn't direct them to further resources for help (Figure 12).

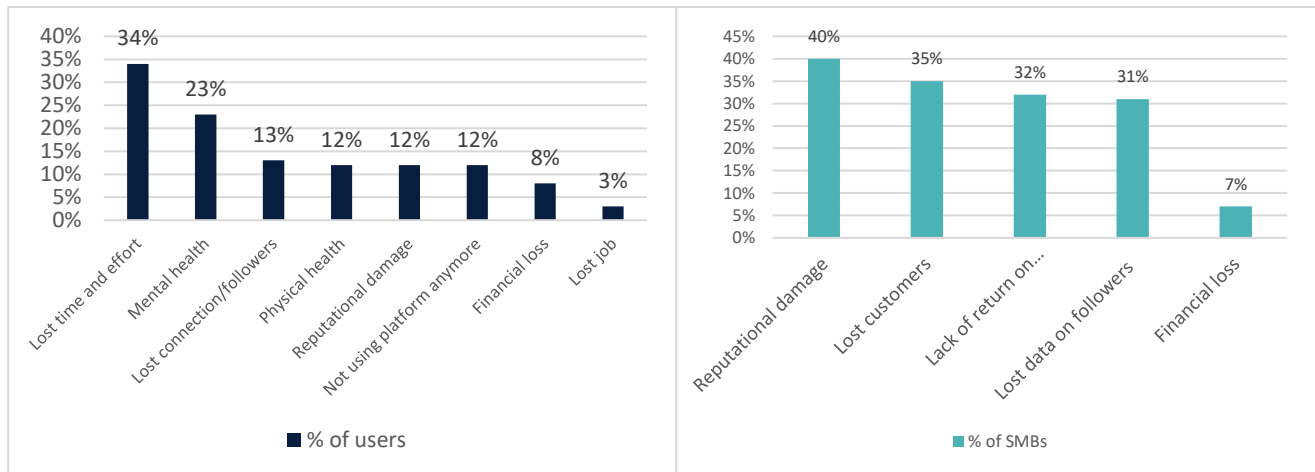
Business users were less likely to have issues with the platform's IDR process, potentially because they can have higher engagement with platforms. Notably, 30 per cent of businesses said they first contacted the platform via a platform representative, such as a personal account manager, which could indicate that they received more personalised service (and therefore greater transparency, explanations and referrals) that consumers throughout the process.

Figure 12. Users who received outcomes still felt that the platform could communicate better

Inefficient dispute resolution processes cost Australians \$3.7 billion in lost time in 2020

In 2020, 23 per cent of consumers who took action invested a lot of time and effort and suffered mental health impacts as a result of the issue they experienced and their attempts to address it. 40 per cent of SMBs suffered reputational damage to their business and 35 per cent of SMBs lost customers, as demonstrated in Figure 13.

Figure 13. Consumers and SMBs suffered a range of adverse consequences as a result of online issues and the dispute resolution process



Most concerning, however, were the financial costs of issues on digital platforms. Of the SMBs that reported a financial loss (7 per cent), the average amount was \$8,855.²⁸ This equates to \$101 million across all SMBs in 2020 and \$2.5 million in lost business tax revenue. Similarly, of the 8 per cent of consumers who reported a financial loss, the average amount was \$1,353. This equates to \$87 million across the population in 2020.

Both consumer and SMB financial losses were in addition to the time cost of resolving the issue. Accenture estimates that if a consumer makes a complaint to a platform it can cost them \$523 in lost time, while if they escalate to an external body it can cost them \$701 in lost time. If a business were to do the same, it would cost them \$1,797 to go to a platform, and \$2,326 to go to an external body (noting that business costs include both a staff member's time and their wages). This equates to \$3.7 billion in lost time across the population in 2020 - \$1.2 billion for consumers and \$2.5 billion for SMBs. There are other costs in addition to the \$3.7 billion in lost time that are difficult to quantify, such as the opportunity cost, lost customers and reputational damage to businesses.

Many un-actioned issues are potentially high-cost issues, such as scams and fake reviews

In 2020, consumers experienced 622,000 issues they left un-actioned, while SMBs experienced 115,000. Both consumers and SMBs reported that 1 in 4 un-actioned issues were spam, which aligns with the most common reason why un-actioned issues weren't reported – they didn't think it would change anything (37 percent and 25 per cent respectively).

s47C - deliberative processes

²⁸ This amount includes the direct cost to the business only and doesn't include the income from lost customers or poorly performing ads.

Chapter 5: The existing external escalation ecosystem

Chapter Overview

Some complaints made by users are not resolved by the internal dispute resolution processes of digital platforms. In these cases, consumers and businesses expect that there are third parties who can advocate on their behalf or support them to resolve the issue.

This chapter provides an overview of the current functions and powers of existing external bodies to identify where there are existing pathways for both individuals and small businesses to externally escalate the issues considered in this report (in-scope issues listed in Figure 9), and to understand where there are gaps.

This chapter uses the terminology ‘external escalation’ rather than ‘external dispute resolution’ because not all of the bodies examined have power to resolve disputes. However, complaints and disputes may still be reported to them.

Bodies that do not have formal dispute resolution powers may still be able to assist by advocating on behalf of, or assisting, a complainant, or by using data from their complaint to better direct resources when tackling systemic issues.

For those bodies that do resolve disputes, there are a range of different ways through which this might occur. For example, the body may perform or refer a complainant to alternative dispute resolution (ADR). This can include non-binding ADR such as mediation, or binding forms such as arbitration. The body may have legislated compliance powers aimed at encouraging companies to adhere to the legislation it administers. Common compliance powers include enforceable undertakings and public notices of failure to comply. Other enforcement powers, which may need to be pursued through the court system, can include fines, injunctions, damages or compensation, other orders such as disqualification orders or adverse publicity orders, and criminal penalties.

The bodies examined include:

- Australian Small Business and Family Enterprise Ombudsman (ASBFEO);
- Australian Communications and Media Authority (ACMA);
- Australian Cyber Security Centre (ACSC);
- State small business bodies;
- Australian Competition and Consumer Commission (ACCC);
- State and territory consumer protection bodies;
- Office of the eSafety Commissioner; and
- Office of the Australian Information Commissioner (OAIC).

These bodies were examined because their remit includes or is relevant to in-scope issues experienced by individuals or small businesses that use digital platforms and they form part of the existing ecosystem of possible external escalation pathways.

Functions and Powers

The following table sets out an overview of the functions of the examined bodies as they relate to in-scope issues, as well as the formal powers conferred on them to resolve or assist in the resolution of those issues. Further detail is at **Attachment D**.

External body	In-scope issues within remit	Functions and powers
Australian Small Business and Family Enterprise Ombudsman	Any issue experienced by a small business where an activity, project, decision or recommendation, or alteration of, failure or refusal to do any of those things affects the small business in trade or commerce.	To make recommendations about how a dispute may be managed, including recommending that an ADR process be used. ²⁹ ASBFEO cannot refer to arbitration or court procedures. Where a party refuses to engage in or withdraws from an ADR process that has been recommended by the ASBFEO, the ASBFEO may publicise that fact. ³⁰ ASBFEO has information gathering powers to assist in exercising its assistance function.
Australian Communications and Media Authority	Spam that falls under the definition in the Spam Act 2003 – ‘unsolicited commercial electronic messages’.	Users can make complaints about spam to ACMA, following which ACMA may contact the sender about its responsibilities under the Spam Act and may investigate serious or ongoing issues. People can also report spam to ACMA, which allows ACMA to identify spam trends and potential compliance issues.
Australian Cyber Security Centre	Issues amounting to cybercrimes – hacking, fake accounts and scams where they amount to identity theft or online fraud.	ACSC receives reports of cybercrime but has no power to deal with complaints itself and refers them to the appropriate police jurisdiction for assessment.
State small business bodies (Vic, NSW, WA, Qld)	The remit, functions, and powers of each State body are different and defined by the body’s establishing legislation. For example, the Victorian Small Business Commission (VSBC) can receive and investigate complaints by small business regarding unfair market practices or commercial dealings, and provide ADR between the parties involved in such a complaint. ³¹ The Commission can also provide ADR to small businesses involved in disputes. ³² Under section 3 of the VSBC Act, “dispute” means a contractual or commercial dispute between a small business and another business, or another body referred to in that section. ADR is defined to include mediation and preliminary assistance only. ³³	
ACCC and State and territory consumer protection bodies (ACL regulators)	The Australian Consumer Law (ACL) within the <i>Competition and Consumer Act 2010</i> (CCA) contains the following relevant provisions: protections against unfair contract terms in standard form consumer and small business contracts;	While it has the power to do so, the ACCC does not currently resolve individual consumer complaints. All ACL regulators are less likely to pursue enforcement where the issue is an isolated event. ³⁴ ACL regulators would only have powers to assist if they believe an issue constitutes a breach of the ACL (or the CCA more broadly for the ACCC). They cannot make a decision as to whether the law has in fact been breached, this must be determined by a court. There are, however, a number of compliance options that do not require a court to determine that a breach has occurred. These include enforceable

²⁹ ASBFEO Act s 71.

³⁰ ASBFEO Act s 74.

³¹ *Small Business Commission Act 2017* (Vic) s 5(2)(c).

³² *Small Business Commission Act 2017* (Vic) s 5(2)(e).

³³ *Small Business Commission Act 2017* (Vic) s 3.

³⁴ [ACCC Compliance and Enforcement Policy](#)

External body	In-scope issues within remit	Functions and powers
	<p>protections against misleading or deceptive conduct and unconscionable conduct;</p> <p>protection against other unfair business practices; and</p> <p>consumer guarantees when purchasing goods and services.</p> <p>It is possible that all in-scope issues except spam could represent breaches of ACL provisions.</p>	<p>undertakings, substantiation notices and public warning notices.</p> <p>Other remedies that require a court to be satisfied that a breach has occurred, or will occur, include:</p> <p>Civil pecuniary penalties</p> <p>Injunctions</p> <p>Damages</p> <p>Compensation orders</p> <p>Adverse publicity orders</p> <p>Disqualification orders</p> <p>Declarations</p> <p>Non-punitive</p> <p>Redress for non-parties</p> <p>Other orders to vary or void contracts.</p> <p>In practice these powers are reserved for significant and systemic breaches, not for individual complaints.</p>
Office of the eSafety Commissioner	Nil	Currently only has power to deal with out-of-scope issues; but receives complaints about hacking and fake accounts, fake reviews, scams, issues around platform complaint handling policies, and account and content removal and procedures. Relies upon informal powers and informal relationships with platforms in responding to these complaints.
Office of the Australian Information Commissioner	Nil	Nil

s47C - deliberative processes

s47C - deliberative processes



s47C - deliberative processes

s47C - deliberative processes

s47C - deliberative processes

Glossary

Term	Definition
ACCC	Australian Competition and Consumer Commission
Accenture Report	Accenture authored report commissioned by the Department to survey Australians, and to better understand the size and scope of issues related to the EDR Scheme Feasibility Study
ACL	Australian Consumer Law (schedule 2 of the <i>Competition and Consumer Act 2010</i> (Cth))
ACMA	Australian Communications and Media Authority
ACSC	Australian Cyber Security Centre
Ad tech	Ad tech is a common abbreviation for ‘advertising technology’. It refers to intermediary services involved in the automatic buying, selling and serving of some types of display advertisements
ADR	Alternative dispute resolution
Advisory Panel	Advisory Panel to consult with other government agencies and key industry stakeholders on EDR Scheme Feasibility Study
AFCA	Australian Financial Complaints Authority
AI	Artificial intelligence – the ability of computer software to perform tasks that are complex enough to simulate a level of capability or understanding usually associated with human intelligence
Algorithm	A sequence of instructions that performs a calculation or other problem-solving operation when applied to defined input data. In this report ‘algorithm’ generally refers to the algorithms used by platforms to rank and display content on their services
App	Application—A software program that performs functions online or on a device
ASBFEO	Australian Small Business and Family Enterprise Ombudsman
CCA	<i>Competition and Consumer Act 2010</i> (Cth)
DIGI	Digital Industry Group Inc
DITRDC	Department of Infrastructure, Transport, Regional Development and Communications
DPI	Digital Platforms Inquiry—conducted by the ACCC into digital search engines, social media platforms and other digital content aggregation platforms, and their effect on media and advertising services markets
DPI Final Report	The final report for the Digital Platforms Inquiry, published on 26 July 2019
DPSI	Digital Platform Services Inquiry 2020-2025—The ACCC’s five-year inquiry into the supply of digital platform services
EC	European Commission
EC	European Commission
EDR	External dispute resolution
EU	European Union

Term	Definition
FOB	Facebook Oversight Board
IDR	Internal dispute resolution
iOS	Apple's operating system for devices including the iPhone. The iPad runs iPadOS, which is based on iOS
Machine learning	The ability of some computer software to autonomously improve knowledge and processes through the repetition of tasks, without the manual entry of new information or instructions
MOU	Memorandum of Understanding
Network effects	The effect whereby the more users there are on a platform, the more valuable that platform tends to be for their users
OAIC	Office of the Australian Information Commissioner
P2B Regulation	Platform-to-Business Regulation (EU), which commenced on 12 July 2020
Privacy Act	<i>Privacy Act 1988</i> (Cth)
Search engines	Software systems designed to search for information on the World Wide Web, generally returning a curated, ranked set of links to content websites
SMBs	Small and medium-sized businesses
Social media platforms	Online services that allow users to participate in social networking, communicate with other users, and share and consume content generated by other users (including professional publishers)
TIO	Telecommunications Industry Ombudsman



Australian Government

Department of Infrastructure, Transport,
Regional Development and Communications

COMMUNICATIONS AND MEDIA / ONLINE SAFETY, MEDIA AND PLATFORMS/ PLATFORMS AND NEWS

International Approaches to Regulating Dispute Resolution Processes for Digital Platforms

External Dispute Resolution Pilot Scheme Feasibility Study: Report 1

July 2021

© Commonwealth of Australia 2021

Ownership of intellectual property rights in this publication

Unless otherwise noted, copyright (and any other intellectual property rights, if any) in this publication is owned by the Commonwealth of Australia (referred to below as the Commonwealth).

Disclaimer

The material contained in this publication is made available on the understanding that the Commonwealth is not providing professional advice, and that users exercise their own skill and care with respect to its use, and seek independent advice if necessary.

The Commonwealth makes no representations or warranties as to the contents or accuracy of the information contained in this publication. To the extent permitted by law, the Commonwealth disclaims liability to any person or organisation in respect of anything done, or omitted to be done, in reliance upon information contained in this publication.

Creative Commons licence

With the exception of (a) the Coat of Arms; (b) the Department of Infrastructure, Transport, Regional Development and Communications photos and graphics; and (c) [OTHER], copyright in this publication is licensed under a Creative Commons Attribution 4.0 Australia Licence.

Creative Commons Attribution 4.0 Australia Licence is a standard form licence agreement that allows you to copy, communicate and adapt this publication provided that you attribute the work to the Commonwealth and abide by the other licence terms.

Further information on the licence terms is available from <https://creativecommons.org/licenses/by/4.0/>

This publication should be attributed in the following way: © Commonwealth of Australia 2021

Use of the Coat of Arms

The Department of the Prime Minister and Cabinet sets the terms under which the Coat of Arms is used. Please refer to the Commonwealth Coat of Arms - Information and Guidelines publication available at <http://www.pmc.gov.au>.

Contact us

This publication is available in hard copy or PDF format. All other rights are reserved, including in relation to any departmental logos or trade marks which may exist. For enquiries regarding the licence and any use of this publication, please contact:

Director – Creative Services
Communication Branch
Department of Infrastructure, Transport, Regional Development and Communications
GPO Box 594
Canberra ACT 2601
Australia

Email: publishing@infrastructure.gov.au

Website: www.infrastructure.gov.au

Table of Contents

1.	Executive Summary	6
1.1	European Union	6
1.2	United Kingdom	7
1.3	North America, New Zealand, Singapore, and other	7
2.	Introduction	9
2.1	Purpose	9
2.2	Scope of disputes	9
2.3	Clarification of dispute resolution terminology	10
3.	European Union	11
3.1	Digital Services Act	11
3.1.1	Who it applies to	11
3.1.2	User redress provisions	12
3.1.3	Other key features	13
3.1.4	Analysis	16
3.2	Platform-to-Business Trading Practices Regulation	16
3.2.1	Who it applies to	17
3.2.2	User redress provisions	18
3.2.3	Analysis	20
3.3	Member State regulations	21
3.3.1	Germany	21
3.3.2	Austria	22
4.	United Kingdom	23
4.1	Draft Online Safety Bill	23
4.1.1	Who and what it applies to	23
4.1.2	Key features	23
4.1.3	User protections	25
4.1.4	Role of the regulator	28
4.1.5	Analysis	28
5.	North America	30
5.1	United States	30
5.2	Canada	31
5.3	Mexico	32
6.	New Zealand and Singapore	33
6.1	New Zealand	33
6.2	Singapore	33
7.	Other Standards and Guidelines	34

7.1	Internet Governance Forum	34
7.2	Santa Clara Principles	34
7.3	OECD's Recommendation on Consumer Protection in e-Commerce	35
8.	Comparison and Analysis	36
8.1	Analysis	36
8.2	Common elements of international regulatory frameworks	38

Glossary

ACCC - Australian Competition and Consumer Commission

ADR - Alternative dispute resolution. Refers to out-of-court dispute resolution mechanisms including negotiation, mediation, arbitration and ombudsmen.

Digital platforms - General term to describe online intermediary services, online intermediation services, and online search engines.

DPI - Digital Platforms Inquiry

Digital Services Act (DSA) - Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC.

EDR - External dispute resolution. Refers to ADR mechanisms that involve a third party to assist or facilitate the resolution of a dispute.

IDR - Internal dispute resolution. Refers to internal processes and systems of companies designed to deal with complaints by users regarding the provision of their services.

Online intermediary services - In relation to the European Union Digital Services Act, online intermediary services include services offering network infrastructure, such as internet access providers and domain name registrars; hosting services such as cloud and web hosting services; and online platforms.

Online intermediation services - In relation to the European Union P2B Regulation, refers to information society services that aim to facilitate the initiating of direct transactions between business users and consumers.

Online platforms - In relation to the European Union Digital Services Act, refers to hosting services that both store information provided by users, and disseminate that information to the public at the user's request. Online platforms include online marketplaces, app stores, collaborative economy platforms and social media platforms.

P2B Regulation – Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services

T&Cs - Terms and conditions.

VLOPs - Very Large Online Platforms. In relation to the European Union Digital Services Act, refers to online platforms with at least 45 million average monthly users within the European Union, being 10% of the population of the Union.

1. Executive Summary

This report considers international developments in government intervention regarding the dispute resolution processes of digital platforms and aims to understand the scope and nature of regulatory intervention around the world in this area.

It explores the approaches taken in the European Union (EU), the United Kingdom (UK), the United States (US), Canada, Mexico, New Zealand and Singapore.

1.1 European Union

The EU is using a staged approach to address a variety of negative consequences for consumers and business users, arising from the functioning of digital platforms.

Firstly, the Regulation on Platform-to-Business Trading Practices (P2B Regulation), adopted in 2020, addresses issues stemming from the dominant position of online intermediary service providers in contract negotiation with business users.

The P2B Regulation has addressed a number of matters, including a lack of redress possibilities, arising from imbalances in bargaining power between ‘online intermediation service’ providers and business users. Reliance by business users on intermediation services and search engines to reach potential consumers has increased significantly. As a result, business users, particularly micro, small and medium enterprises, are often unable to negotiate the terms and conditions that govern their contractual relationship with a service provider. Where terms are imposed unilaterally, they may lack sufficient, fair or transparent redress options in the case of disputes between parties.

P2B Regulation enhances user redress options by:

The Regulation on Platform-to-Business Trading Practices seeks to remedy the consequences of the power imbalance between service providers and business users by:

- Requiring minimum standards for terms and conditions, including:
 - Internal complaint-handling systems; and
 - Commitment to engage in good faith with named mediators.
- Statements of reasons for decisions to restrict, suspend or terminate use of services.

Secondly, the European Commission proposed a package of legislation in late 2020, comprising the Digital Services Act (DSA) and Digital Markets Act (DMA). This report focuses on the DSA, as it proposes obligations on providers to establish user redress mechanisms. The DSA posits that ‘online intermediary services’, defined at 3.1.1, have significantly evolved in the last two decades, becoming ubiquitous and necessary for participation in modern society. The potential impact of unilateral decisions by providers to limit individuals’ use of a service is therefore great, as is the risk of harm to users due to misuse of a service. User redress mechanisms and other requirements are proposed in response to the increased role of services in everyday life, making the responsibilities of providers to act in a fair and transparent fashion commensurate with their potential impacts on users.

Digital Services Act enhances user redress options by:

- Requiring some minimum standards for T&Cs, including:
 - Information on any restrictions imposed on use of the service; and
 - Information on content moderation policies, procedures, measures and tools.
- Requiring providers to establish internal complaint-handling systems.
- Requiring providers to engage with certified out-of-court dispute settlement bodies in relation to certain disputes.

- Imposing transparency reporting requirements.
- Requiring very large online platforms to assess the systemic risks arising from the use of their service, and to take measures to mitigate such risks.

Additionally, some Member States, including Germany and Austria, have enacted or drafted their own measures to combat harms arising from the use of digital platforms. These are mainly intended to address illegal content such as hate speech, rather than the broader range of issues addressed in the P2B Regulation and DSA.

1.2 United Kingdom

On 12 May 2021, the UK government released a draft of its Online Safety Bill. The draft Bill establishes a regulatory framework to address harmful content online, giving effect to the UK government's policy position presented in response to the 2019 Online Harms White Paper.

The draft Online Safety Bill imposes a number of statutory duties on providers of user-to-user services and search engines. While these include duties to operate reporting and redress mechanisms for certain types of complaints, the UK Government Response to the Online Harms White Paper specified that it does not intend to establish an independent resolution mechanism.

Alongside meeting their duty of care, companies in scope may also be required to provide transparency reporting, respond to information requests, use automated technology to remove illegal content, and pay an annual industry fee. The draft Bill will expand the remit of the UK's existing telecommunications regulator, giving it monitoring and enforcement powers.

Most relevant to the purpose of this report, the draft Online Safety Bill includes specific legal duties to have effective and accessible user reporting and redress mechanisms for certain types of content and activity which service providers have to address as part of their duties of care.

Notably, the UK government has made clear that it will not mandate specific forms of redress and it does not intend to establish an independent resolution mechanism, such as an ombudsman or certified alternative dispute resolution scheme.

The draft Online Safety Bill also enhances user protections by setting out a number of elements that must be included in providers' terms and conditions (T&Cs).

1.3 North America, New Zealand, Singapore, and other

Legislation touching on dispute resolution has been proposed or is planned to be proposed in each of the US, Canada and Mexico. However, none of these proposals address the range of disputes covered by the EU's P2B Regulation or proposed DSA, or by the UK's Online Harms White Paper.

Following terrorist attacks in Christchurch in 2019, New Zealand co-created the Christchurch Call to Action setting out principles for digital platforms and governments to follow with the aim of eliminating terrorist and violent extremist content online. However, the New Zealand government has not planned or proposed any regulation of digital platforms.

The Singaporean government takes a light-touch approach toward regulating digital platforms particularly in terms of dispute resolution. However, platforms are subject to the Protection from Online Falsehoods and Manipulation Act, which gives the government significant powers to issue correction notices to individuals and platforms, and direct individuals to stop communication.

Additionally, number of bodies have issued guidelines or standards to assist platforms and governments to create effective and efficient user redress processes.

For example, in 2019 the Dynamic Coalition on Platform Responsibility sub-committee of the United Nations Internet Governance Forum published a document titled 'Best practice on Platforms' Implementation of the Right to an Effective Remedy'. The document outlined best practice based on solutions that effectively balance the protection of users' rights with considerations of the viability of platforms' business models. It sets out a recommendations for implementing and maintaining alternative appeals mechanisms.

In 2018, the Santa Clara Principles on Transparency and Accountability in Content Moderation were created at the Content Moderation at Scale conference. The principles provide a set of baseline standards or initial steps that companies engaged in content moderation should take to provide meaningful due process to impacted speakers and better ensure that the enforcement of their content guidelines is fair, unbiased, proportional, and respectful of users' rights.

Lastly, in 2016, the Organisation for Economic Co-operation and Development (OECD) published a recommendation on the protection of consumers in the context of e-commerce. The Recommendation applies to business-to-consumer electronic commerce, including commercial practices through which businesses facilitate consumer-to-consumer transactions.

2. Introduction

2.1 Purpose

The Australian Competition and Consumer Commission's (ACCC) Digital Platforms Inquiry Final Report recommended that, to ensure that consumers and small businesses have appropriate avenues for complaint and dispute resolution, the internal dispute resolution systems of digital platforms should comply with a minimum standard and that an Ombudsman scheme should be established to resolve disputes. The Government agreed to develop a pilot external dispute resolution (EDR) scheme, which would inform whether an Ombudsman would be established. It also agreed to assess improvements in the internal dispute resolution (IDR) processes of digital platforms.

Since the ACCC's Report was released in December 2019, there have been numerous developments in the IDR frameworks and policies of digital platforms. Consideration of the adequacy of platforms' current IDR frameworks should therefore take place before deciding whether to establish a pilot EDR scheme, in order to understand whether unresolved disputes remain a substantial issue. International developments and best practice in dispute resolution should also be considered.

To this end, the Department has undertaken an EDR scheme feasibility study. The study aims to gather information on the prevalence and nature of disputes between individuals and small businesses, and digital platforms. The outcome of the study will be advice to Government as to whether an EDR scheme is necessary, and if so, what form it should take.

This report considers international developments in government intervention regarding the dispute resolution processes of digital platforms and aims to understand the scope and nature of regulatory intervention around the world in this area.

2.2 Scope of disputes

This report is a broad investigation of actions by international governments requiring providers of digital platforms to establish or engage in dispute resolution mechanisms, both internal and external. The type of disputes that such mechanisms are aimed at resolving have not been specified.

The ACCC's Report left the scope of disputes that may be subject to its recommended ombudsman scheme quite broad. It stated that the nature of relevant disputes would be determined following consultation with stakeholders, but that they may include:¹

- Complaints or disputes from businesses relating to the purchase of advertising from digital platforms;
- Complaints or disputes from businesses that consider digital platforms' representations about the performance or likely performance of purchased advertising to be inaccurate or unsubstantiated; and
- Complaints or disputes from consumers, including in relation to scams and the removal of such content.

While the first two categories of dispute are narrower and relate specifically to advertising, the third category can be interpreted as very broad, seemingly encompassing any complaints from consumers, of which scam content is one area. Other complaints from consumers that could be addressed by a dispute resolution scheme include those about platforms taking decisions which affect users' ability to access services, or to remove content.

What disputes do other frameworks look at?

Broadly, the disputes and complaints that fall within the scope of international dispute resolution frameworks, both enacted and proposed, fall into the following two categories:

- Decisions by providers to restrict, suspend or terminate use; and
- Failures of providers to fulfil regulatory duties, including meeting minimum standards relating to platforms' terms and conditions, data handling, and algorithmic transparency.

In the European Union's (EU) proposed Digital Services Act, the disputes that fall within the scope of the internal complaint-handling system and out-of-court settlement provisions include decisions to restrict or disable access to

¹ Australian Competition and Consumer Commission (ACCC), *Digital Platforms Inquiry Final Report*, Australian Government, 2019, p 27.

content; suspend or terminate provision of the service or part thereof; and decisions to suspend or terminate a user's account.

In the EU's in force Regulation on Platform-to-Business Trading Practices, disputes may be brought before the internal complaint-handling system or escalated to mediation. The following issues may form the subject of those disputes, provided the business of the user is affected by them:

- non-compliance with the Regulation;
- technological issues in provision of the service; and
- measures taken by, or the behaviour of, the provider relating to provision of the services.

The latter would presumably include decisions to restrict, suspend, or terminate use of the service.

The United Kingdom's (UK) draft Online Safety Bill sets out that companies will be required to have reporting and complaints procedures for the types of content and activity they must address as part of their duties of care. This depends on the categorisation of the service, but can include harmful content; decisions to warn, suspend, ban or otherwise restrict use of the service; non-compliance with safety duties; and non-compliance with duties to protect freedom of expression and privacy.

In Canada's Bill C-11, recourse options for users of platforms are available only in regard to the proposed regulatory duties which relate to privacy and the handling of personal data.

A Bill submitted to the United States (US) Senate in June 2020 proposes to require internal complaint-handling systems that deal with good faith user complaints regarding potentially policy-violating content; illegal content or activity; or decisions by the provider to remove content.

2.3 Clarification of dispute resolution terminology

For the purposes of this report, 'external dispute resolution' refers to the subset of alternative dispute resolution (ADR) mechanisms that utilise a third-party to facilitate or assist with the resolution of disputes. Conversely, internal dispute resolution (IDR) refers to the processes that digital platforms employ within their own business to receive and resolve complaints by users.

In its DPI Report, the ACCC refers to 'external' dispute resolution systems. In order to obtain a complete understanding of international government intervention in digital platform dispute resolution, this paper will consider all types of ADR. 'Alternative' dispute resolution refers to methods of resolving disputes outside of traditional avenues such as courts and tribunals. Use of an ADR mechanism does not necessarily preclude parties from subsequently enforcing their rights through external methods, such as in court. The following are commonly used ADR methods:²

- **Negotiation:** If an agreement is reached, it may be enforceable as a contract. There is no neutral third-party involved – negotiation is between the parties themselves on a voluntary basis.
- **Arbitration:** If parties agree to engage in arbitration, they present arguments and evidence to the arbitrator who makes a binding determination.
- **Mediation:** The role of the mediator is to assist in identifying the disputed issues, developing options, considering alternatives and trying to reach an agreement. The mediator does not have an advisory or determinative role in regard to the content of the dispute or the outcome. If an agreement is reached, it may be binding as a contract.
- **Ombudsman:** Ombudsmen can have information gathering and investigation powers, and may have authority to decide the resolution of a complaint, make recommendations and make binding assessments.

² National Alternative Dispute Resolution Advisory Council, [Your Guide to Dispute Resolution](#) [online document], Attorney-General's Department, 2012, accessed 16 March 2021.

3. European Union

3.1 Digital Services Act

In December 2020, the European Commission proposed a legislation package to establish a comprehensive set of rules for all digital services including social media, online market places, and other online platforms operating in the EU. The package comprises the Digital Services Act (DSA) and Digital Markets Act (DMA).

The DMA is designed to address the consequences of certain platforms acting as digital “gatekeepers” to the single market.

The DSA is designed to address the significantly different role played by online intermediaries since the eCommerce Directive was adopted in 2000. Importantly, it acknowledges that there are a number of very large platforms that have become ‘quasi-public spaces’ for information sharing and trade. The DSA represents recognition that *ex ante* regulation of online intermediary services is necessary to mitigate the risk of harm stemming from the use and design of online services.

The proposal introduces safeguards to allow citizens to freely express themselves, while enhancing user agency in the online environment. The proposal will mitigate risks of erroneous or unjustified blocking of speech and stimulate the freedom to receive information and hold opinions, as well as reinforce a users’ ability to seek redress.

In addition to a number of mandatory requirements aimed at achieving the above, the DSA encourages the drawing up of Codes of Conduct and Standards to facilitate its proper application.

The European Parliament and the Member States will discuss the proposed legislation in the ordinary legislative procedure. If passed, it is unlikely to come into force before 2023.

3.1.1 Who it applies to

The DSA applies to online intermediary services, which includes hosting, caching and ‘mere conduit’ services. The provisions of the DSA apply to online intermediary services in a tiered manner, ensuring that the obligations applicable to each tier are commensurate with the role, size and impact of services provided. Obligations are cumulative – for example, obligations applying only to very large online platforms are additional to those applying to all online platforms. The tiered approach is outlined in the diagram below.

Intermediary services

Services offering network infrastructure, such as internet access providers and domain name registrars.

Hosting services

Such as cloud and webhosting services.

Online platforms

A subset of hosting services which both store information provided by users, and disseminate that information to the public, at the user’s request. This does not include private messaging and email services. It includes online marketplaces, app stores, collaborative economy platforms and social media platforms.

Very large online platforms (VLOPs)

Online platforms with 45 million average monthly users, being 10% of the population of the European Union.

The DSA imposes asymmetric obligations on different types of intermediary services in recognition of the differing levels of impact, both personal and economic, that they have on the lives of users. In relation to the additional obligations for VLOPs, the Commission provided the following justification:

Given the importance of very large online platforms, due to their reach, in particular as expressed in number of recipients of the service, in facilitating public debate, economic transactions and the dissemination of information, opinions and ideas and in influencing how recipients obtain and communicate information online, it is necessary to impose specific obligations on those platforms, in addition to the obligations applicable to all online platforms.

As specified in relevant provisions, micro and small enterprises will not be required to comply with obligations that are disproportionate to their size and ability to comply. Relevant provisions include the requirement to provide internal complaint-handling systems and to engage in out-of-court dispute settlement.

The DSA is intended to apply to all online intermediaries offering services within the European Union, whether they are established inside or outside the Union.

3.1.2 User redress provisions

3.1.2.1 Notice and action mechanisms

The DSA requires providers of **hosting services**, which includes online platforms, to put in place user-friendly, easy to access mechanisms that will allow any individual or entity to notify them of the presence of content on their service that the individual or entity considers to be illegal.

The provider is also required to notify that individual or entity of its decisions in respect of the content to which the notice related, and provide information on the redress possibilities available in respect of that decision.

In addition, Article 19 requires **online platforms** to establish measures to prioritise notices submitted by ‘trusted flaggers’. Trusted flagger status can be awarded, upon application, to entities with particular expertise and competence in detecting illegal content. Such entities must represent collective interests and be independent from any online platforms.

3.1.2.2 Statements of reasons

Article 15 of the DSA requires that, where providers of **hosting services** decide to remove or disable access to content provided by a user, the provider must inform the user of that decision at the latest at the time of the removal or disabling, and provide a clear and specific statement of reasons for that decision.

The statement of reasons must include information about the redress possibilities available to the user in respect of the decision, namely internal complaint-handling mechanisms, out-of-court dispute settlement and judicial redress.

Importantly, the information provided in the statement of reasons must be sufficient to allow the user to effectively exercise the redress opportunities mentioned above.

The requirement to provide a statement of reasons applies irrespective of the reasons for the decision. It appears that providers would therefore be required to provide statements of reasons even when removing or disabling access to content that is manifestly illegal.

3.1.2.3 Internal complaint-handling system

Article 17 of the DSA sets out the requirements for **online platforms** in relation to the provision of an internal complaint-handling system. The system must enable users to submit complaints about the following decisions made on the ground that the information provided by the user is illegal or incompatible with the provider’s T&Cs:

- Decisions to remove or disable access to the information;
- Decisions to suspend or terminate the provision of the service, in whole or in part to the user; and
- Decisions to suspend or terminate the user’s account.

Online platforms must ensure that their internal complaint-handling system is easy to access, user-friendly and allow users to submit sufficiently precise and substantiated complaints. They must also handle complaints in a timely, diligent

and objective manner, and inform complainants of the decision they take in respect of the complaint without delay. This notice of decision must include information about other redress possibilities, including out-of-court dispute settlement.

Notably, platforms must ensure that decisions relating to complaints are not solely made by automated means.

3.1.2.4 Out-of-court dispute settlement

The disputes to which Article 18, which sets out requirements for out-of-court dispute settlement processes, refers are those decisions subject to the internal complaint-handling process in Article 17. Article 18 applies to online platforms.

Users subject to the decisions listed in Article 17 are entitled to select two out-of-court dispute bodies that have been certified by the Digital Services Coordinator of the Member State in which the body is established. In order to become certified, bodies must demonstrate *inter alia* that they: are impartial and independent from all parties to the dispute; have the appropriate expertise to deal with the relevant issues; and can conduct settlement through electronic communication technology.

Alternatively, Member States may establish out-of-court dispute settlement bodies for the purposes of this Article.

Users may turn to out-of-court settlement after utilising the provider's internal complaint-handling system, where the dispute was unable to be resolved through that process. The platforms are obligated to engage in good faith with the selected body with a view to resolving the dispute, and are bound by decisions of the body.

In respect of fees, where a dispute is decided in favour of the user, the platform must reimburse the user any fees and other reasonable expenses paid in relation to the dispute settlement. Conversely, if the dispute is decided in favour of the platform, the user is not required to pay fees or other expenses incurred by the platform. This incentivises platforms to resolve disputes prior to their escalation to out-of-court dispute settlement.

3.1.2.5 Right to lodge complaint against provider

Under Article 43, users have the right to lodge a complaint against providers of intermediary services alleging an infringement of the DSA. This complaint is lodged with, and assessed by, a Digital Services Coordinator. The powers of Digital Services Coordinators are outlined in 3.1.3.5 below.

3.1.3 Other key features

3.1.3.1 Terms and conditions

Under the DSA, all intermediary services will be required to stipulate in their T&Cs any restrictions imposed on use of the service, in respect of information provided by users. They must also set out any policies, procedures, measures and tools used for the purpose of content moderation, whether it is done algorithmically or by a human.

In addition, where VLOPs use recommender systems in their services, they must set out the main parameters used by those systems in their T&Cs.

3.1.3.2 Risk assessment and mitigation

Many of the provisions in the DSA are designed to recognise that the risks of harm occurring through online intermediary services are created or amplified by the design of the service and its features. The legislation is also intended to recognise that purely consumer or competition law approaches to regulating online platforms, particularly VLOPs, fail to recognise the role they have come to play in modern society and the impact they can have on societal values and human rights, as explained below:

Very large online platforms are used in a way that strongly influences safety online, the shaping of public opinion and discourse, as well as on online trade. The way they design their services is generally optimised to benefit their often advertising-driven business models and can cause societal concerns. In the absence of effective regulation and enforcement, they can set the rules of the game, without effectively identifying and mitigating the risks and the societal harm they can cause.

European Commission

As such, the DSA includes requirements for **VLOPs** to assess any systemic risks arising from the functioning and use of their services. The systemic risks assessed are to include:

- the dissemination of illegal content;
- negative effects on the fundamental rights for private and family life, freedom of expression and information, and of prohibition of discrimination and the rights of the child; and
- intentional manipulation of the service with actual or foreseeable negative effects on protection of public health, civil discourse, or actual or foreseeable effects related to electoral processes and public security.

In assessing these risks, VLOPs are to also consider the contributions that content moderation and recommender systems, and systems for selecting and displaying advertising may make to the risk.

Where a VLOP identifies a systemic risk arising from the functioning or use of its platform, Article 27 requires it to put in place reasonable, proportionate and effective mitigation measures.

3.1.3.3 Transparency reporting

The DSA imposes transparency reporting requirements on all companies subject to the legislation, except those providers qualifying as micro or small enterprises, with substantial reporting obligations applying to VLOPs.

The lowest tier of reporting requirements, applicable to all online **intermediary service** providers except for micro and small enterprises, includes annual reporting on any content moderation engaged in. This includes:

- The number of orders received by Member States, including orders to act against illegal content, and average time needed to respond to those orders;
- The number of notices submitted through the compulsory notice and action mechanisms, and any action taken in response;
- Any content moderation engaged in at the provider's initiative; and
- The number of complaints received through the mandatory internal complaint-handling system, the basis for those complaints, and decisions taken in respect of those complaints.

In addition, **online platforms** must also include information about, *inter alia*, disputes submitted to out-of-court dispute settlement bodies referred to in Article 18; suspension for frequent sharing of manifestly illegal content pursuant to Article 22; and any use of automatic content moderation.

Further, **VLOPs** will be required to report on the required risk assessment and risk mitigation measures implemented pursuant to Articles 26 and 27, and the independent audit report required by Article 28.

3.1.3.4 Other relevant consumer protections

While not subject to the required internal complaint-handling or out-of-court dispute settlement processes in Articles 17 and 18, the DSA implements a number of other provisions designed to protect the interests of users. The provisions outlined below relate directly to the types of issues identified by the ACCC as being potentially subject to an external dispute resolution mechanism in Australia, such as scams and online advertising transparency. The EU's approach is to set transparency requirements that providers must meet, thereby reducing instances in which it is likely that those issues will lead to a dispute.

Online advertising transparency

For advertisements appearing on an **online platform's** interface, the provider must ensure that users can identify, for each specific advertisement displayed to each individual recipient, in a clear and unambiguous manner and in real time:

- That the information displayed is an advertisement;
- The person or entity on whose behalf the advertisement is displayed; and
- Meaningful information about the main parameters used to determine the recipient to whom the advertisement is displayed.

Requiring platforms to display this information alongside all advertisements will allow users to make more informed choices about whether to rely on the information presented, potentially leading to a reduction in the instances of harm caused by scam advertising on platforms.

In addition, **VLOPs** are required to keep a publicly available repository containing a range of information about all advertisements displayed on the platform, for a 12 month period after the advertisement is displayed for the last time. The data required to be included in the repository is set out in Article 30.

Trader traceability

Article 22 is designed to reduce opportunities for bad actors to utilise platforms to the financial detriment of consumers. Where an **online platform** allows consumers to conclude distance contracts with traders, the platform must first obtain certain identifying information about the trader before they can promote or offer products or services to consumers. The information that traders must provide includes their name, address, telephone number and email address; bank account details where the trader is a natural person; the registration number or equivalent if the trader is registered in a trade register; and a self-certification by the trader committing to only offer products or services that comply with applicable EU law.

Upon receipt of this information from traders, platforms must make reasonable efforts to assess its reliability. If a trader fails to correct or complete the information after a request from the provider, the provider may suspend provision of its service until the trader complies.

Article 22 provides an example of how requiring platforms to include user protection in the design of their systems and processes would lead to a reduction in harms occurring to users, rather than only requiring platforms to submit to external dispute resolution after a harm has occurred. Both this Article and those promoting online advertising transparency, put the responsibility on providers to ensure that their platforms are not misused, rather than putting the onus on users to pursue redress once they encounter an issue.

Algorithmic transparency

Article 29 requires that **VLOPs** that use recommender systems must set out in their T&Cs the main parameters used by the recommender systems, as well as options for users to modify or influence those main parameters. They must also provide easily accessible functionality on their interface, allowing users to select and modify their preferred option for each recommender system that determines the relative order of information presented to them. At least one option must not be based on profiling, within the meaning of Article 4 (4) of Regulation (EU) 2016/679.

Providing options to modify or influence the main parameters used to recommend content will give users more control over the information that is presented to them. Additionally, giving users more information about *why* certain information is being presented to them may allow them to avoid content they do not wish to encounter, including scam content. It also gives users a means to control which aspects of their identity are used to recommend content, reducing the potential for algorithmic recommendation to result in bias or discrimination.

3.1.3.5 Application and enforcement

Member States are to entrust one or more competent authorities with supervisory and enforcement tasks relating to the application of the DSA. Competent authorities may be new or already established, and may, for example, be sector specific regulators or consumer protection authorities.

Member States must designate a competent authority as 'Digital Services Coordinator', responsible for all matters relating to the application and enforcement of the DSA in that Member State.

Digital Services Coordinators have the power to:

- Require the provision of information relating to a suspected infringement of the DSA;
- Accept and make binding commitments from providers in relation to their compliance with the DSA;
- Order cessation of infringements, and impose remedies to end infringements;
- Impose fines of up to 6% of annual income or turnover, for failure to comply;
- Impose periodic penalties of up to 5% of average daily turnover, to ensure timely cessation of infringements or provision of information relating to suspected infringement; and
- Adopt interim measures to avoid the risk of serious harm.

Digital Services Coordinators will be advised by the European Board for Digital Services, established by Article 47. The Board is an independent advisory group made up of Digital Service Coordinators, intended to assist with the supervision of providers of intermediary services.

3.1.4 Analysis

The DSA package, consisting of both the DSA and DMA, aims to streamline the various instruments relating to digital platforms introduced to complement the eCommerce Directive since 2000. In so doing, it takes a holistic approach and aims to address the root cause of a variety of issues, which all contribute to the protection of users, rather than continuing to introduce *ex post* regulations.

In addition, the DSA represents a shift in perspective in the aim of regulation of digital platforms.³ It recognises that there is an emerging genre of issues that arise from the ubiquity of digital platforms in everyday life, and which fall outside the scope of competition or consumer law fixes. As the role of platforms has grown to encompass most aspects of modern life, the DSA is designed to fulfil a perceived regulatory gap that provides sufficient accountability and transparency around the actions of platforms to reflect their reach and influence.

While the DSA aims to require platforms to take more responsibility for this increased role in society and ability to impact the lives of individuals, other issues stemming from the dominance of major platforms are addressed from a competition perspective through the Digital Markets Act.

The DSA package is useful because, instead of addressing discrete issues through narrow targeted means, it aims to address the underlying cause of the issue and is therefore applicable more broadly to a range of scenarios. For example, the DSA recognises that there are common underlying causes of issues such as scam advertisements, dissemination of harmful content, and user dissatisfaction with treatment by platforms. These include a lack of transparency in advertising and recommender systems, a lack of notification mechanisms to bring attention to issues, and a lack of redress mechanisms that allow users to hold platforms to account. By obligating online intermediary services to build these elements into the design of their service, the DSA may reduce the need for regulation in reaction to specific instances of harm.

Stakeholder Feedback

A feedback period on the adoption of the DSA by the European Commission closed 31 March 2021. 138 submissions were received, including from Microsoft, Etsy, Booking.com, and Snap Inc. These platforms were overall supportive of the EU's policy objectives, however, a number suggested greater proportionality in the categorisation of VLOPs and recognition that some companies offer multiple services with differing business models.

In 2020, a number of digital platforms also provided submissions in response to the Inception Impact Assessment, including Apple, Match Group, eBay, Shopify, Google, Booking.com, Microsoft, and Facebook.

Many focused on preserving the limitations to intermediary liability, and how this allows intermediaries to benefit consumers through increased flow of information online. The DSA does preserve the framework of exemptions from liability for providers of intermediary services laid down in the eCommerce Directive, where the intermediaries do not have knowledge of illegal content or activity.⁴

Broadly, platforms supported the clarification of the responsibilities of online service providers, the harmonisation of notice and takedown procedures, and a systemic approach to oversight. However, many also suggested that the voluntary efforts of platforms should be considered when reflecting on the need for an *ex ante* regulatory framework. As the European Commission decided to propose an *ex ante* regulatory framework, it can be assumed that the voluntary measures of platforms were considered inadequate to achieve the objectives set out in the DSA.

3.2 Platform-to-Business Trading Practices Regulation

The P2B Regulation came into force in July 2019, and entered into application in July 2020.

Its purpose is to ensure that business users of 'online intermediation services', defined below at 3.2.1, and corporate website users of online search engines are granted appropriate transparency, fairness and effective redress possibilities.

The P2B Regulation recognises that business users increasingly depend upon online intermediation services and online search engines to reach consumers and increase traffic to their sites. Consequently, the actions of online intermediary

³ Hans Schulte-Nolke et al., [The legal framework for e-commerce in the Internal Market](#), Directorate-General for Internal Policies, European Union, 2020, p 33.

⁴ Digital Services Act, Recital 16.

service providers and online search engines can significantly affect the commercial success of business and corporate website users. This increased reliance of businesses, particularly micro, small and medium-sized enterprises, on online intermediation services has created an imbalance in bargaining power. As such, providers have been able to unilaterally stipulate the terms of their relationships with business users, with relatively little oversight and transparency.

Provisions within the P2B Regulation seek to address the situation where the power imbalance between providers and business users results in limited possibilities to seek redress where the unilateral actions of providers lead to disputes.⁵

3.2.1 Who it applies to

The P2B Regulation applies to online intermediation services and online search engines through which business users and corporate website users, respectively, offer goods or services to consumers. The Regulation defines online intermediation services as:

...information society services,⁶ which are characterised by the fact that they aim to facilitate the initiating of direct transactions between business users and consumers, irrespective of whether the transactions are ultimately concluded online, on the online portal of the provider of online intermediation services in question or that of the business user, offline or in fact not at all, meaning that there should be no requirement for any contractual relationship between the business users and consumers as a precondition for online intermediation services falling within the scope of this Regulation.

P2B Regulation, Recital 10

Note that this definition differs from the terminology used in the Digital Services Act. The DSA uses ‘online intermediary service’ as opposed to ‘online intermediation service’, and this refers to the broadest category of services within its scope, as outlined above at 3.1.1.

The P2B Regulation applies to online intermediation services that provide services to business users through a contractual relationship. In order to achieve its purpose of protecting business users from an imbalance in bargaining power, the P2B Regulation applies only where the T&Cs of the contract governing the relationship between the business user and the provider are unilaterally determined. Whether T&Cs are unilaterally determined is evaluated on a case-by-case basis, according to a number of factors.⁷

The P2B Regulation does not apply to online advertising tools and online advertising exchanges that are not provided with the aim of facilitating the initiation of direct transactions with consumers and that do not involve a contractual relationship with consumers. Therefore, the P2B Regulation may not cover the first two types of disputes identified by the ACCC as being potentially subject to an EDR scheme, outlined above at 2.2. These relate to the purchase and performance of advertising.

‘Business users’ are any private individual that is acting in a commercial or professional capacity, or any legal person, who offers goods or services to consumers through online intermediation services.

‘Consumers’ are defined as any natural person who is acting for purposes that are outside this person’s trade, business, craft or profession.

The P2B Regulation also applies to online search engines, though not all provisions apply to both online intermediation service and search engines.

Online intermediation services include:

- E-commerce marketplaces on which a commercial transaction between a customer and a business user takes place, such as Amazon market place, eBay, Uber and Booking.com, and app stores; and

⁵ DG CONNECT, [Impact assessment of the Proposal for a Regulation of the European Parliament and of the Council on promoting fairness and transparency for business users of online intermediation services](#), European Commission, 2018.

⁶ As defined in Directive (EU) 2015/1535 of the European Parliament and of the Council at Article 1(1)(b).

⁷ EU Digital Services Act, Recital 14.

- Online platforms bringing together business users and consumers with the aim to facilitate a commercial transaction, regardless of whether the transaction is concluded online or offline. This includes Facebook marketplace, Google My Business and price comparison websites.⁸

The P2B Regulation does not apply to purely business-to-business intermediation services which cannot be accessed by consumers, or to peer-to-peer platforms that do not have business users present. It similarly does not apply to payment platforms, such as PayPal, that cannot be used to initiate a transaction.

Some rules for online intermediation services only apply to larger providers. Importantly, and similarly to the Digital Services Act, online intermediation service providers qualifying as small enterprises are exempt from the obligations to set up a complaint handling system and to specify mediators in their T&Cs.

The UK has confirmed that the EU's P2B Regulation continue to apply in the UK following Brexit. The P2B Regulations are enforced in the UK through the [Online Intermediation Services for Business Users \(Enforcement\) Regulations 2020](#).

3.2.2 User redress provisions

3.2.2.1 Minimum standards for terms and conditions

The P2B Regulation achieves its purpose primarily through establishing minimum standards for T&Cs, including a comprehensive list of obligatory T&Cs that online intermediation services must include in unilaterally determined contracts with business users. These include:

- A description of the grounds on which providers may base decisions to suspend, terminate or otherwise restrict the use of its services by a business user;
- Information about any additional distribution channels or affiliate programs used to market goods and services offered by a business user;
- Information about the effect of T&Cs on the intellectual property rights of the business user;
- A description of the main parameters determining ranking and the reasons for the relative importance of those parameters compared to others. Online search engines are to include this information in a publically available description. The Commission has published Guidelines on ranking transparency (2020/C 424/01) to assist with fulfilling this requirement;
- A description of any possibility to influence ranking against any direct or indirect remuneration paid by the business user to the provider;
- A description of any complementary ('ancillary') goods and services providers may propose to consumers alongside the business user's primary offer, and of when a business user may offer its own complementary goods and services through the service;
- Information on how providers treat and rank goods and services offered by themselves or by business users they control compared to those offered by third-party business users;
- Information on how business users can terminate the contractual relationship;
- A description of access the provider may retain to data generated or provided by the business user, after the contractual relationship has terminated;
- A description of data access policies;
- A description of any grounds for restricting the ability of the business user to offer different conditions through other means, such as offering the goods or services at a lower price on another website;
- Information on the internal complaint-handling system, including how business users can avail themselves of it and how it operates. See 3.2.2.3 below; and
- The names of two or more mediators to settle, out of court, any disputes that may arise. See 3.2.2.4 below.

The P2B Regulations also contain notice requirements where a provider intends to change their T&Cs, recognising that sudden changes can significantly disrupt business users' operations. There is a minimum notice period of 15 days prior to any change, subject to some exemptions, allowing business users to make any technical or commercial adaptations necessary to comply with the new T&Cs.

⁸ DG CONNECT, [Impact assessment of the Proposal for a Regulation of the European Parliament and of the Council on promoting fairness and transparency for business users of online intermediation services](#), European Commission, 2018, pp 6-8.

T&Cs must be easy to read and understand, easy to find, and available at all stages of the contractual relationship, including at the pre-contractual stage.

3.2.2.2 Decisions to restrict, suspend or terminate use

Decisions by providers to restrict, suspend or terminate a business users' use of a service can have significant adverse effects on the interests of the user. As such, the P2B Regulation puts in place procedural standards for those decisions.

As mentioned above, the P2B Regulation requires online intermediation services to include grounds for decisions to restrict, suspend or terminate use of their service in their T&Cs.

Pursuant to Article 4, providers must give a statement of reasons for a decision to restrict, suspend or terminate a business user's use of the service. This is intended to allow the user to understand whether there is scope to challenge the decision through the provider's internal complaint-handling system, via mediation, or through the courts. Statements of reasons must refer to:

- The specific facts or circumstances, including contents of third party notifications, that led to the decision; and
- The ground for the decision based on what is listed in the T&Cs.

Statements are required to be made using a durable medium, such as e-mail, which allows users to keep the notice for future reference.

For decisions to restrict or suspend use, the statement of reasons must be supplied prior to or at the time of the decision taking effect. For decisions to terminate the provision of the whole of the service to a given business user, providers must give the user a statement of reasons at least 30 days prior to the termination taking effect. There are exceptions to this requirement, such as where termination is imperative pursuant to a national law, or where the user has repeatedly infringed the applicable T&Cs.

For all three decisions, the provider is obliged to give the user an opportunity to clarify facts and circumstances through the internal complaint-handling framework.

3.2.2.3 Internal complaint-handling system

Under Article 11, all providers of online intermediation services, except small providers, are required to establish an internal complaint-handling system. Providers of small online intermediation services may do so voluntarily.

The system must be open to all business users, including those whose use of the service may have been restricted, suspended or terminated.

Matters about which business users can complain through the internal system are very broadly defined as including the following, so far as they impact the business user:

- Alleged non-compliance with obligations in the P2B Regulation;
- Technological issues relating to the service; and
- Measures taken by, or the behaviour of, the service that relate directly to the services provided.

The measures referred to above would include decisions to restrict, suspend or terminate the provision of a service.

Use of the internal complaint-handling system does not preclude either party from seeking redress through a court or an alternative dispute resolution mechanism.

At least annually, providers are to make publically available information on the functioning and effectiveness of the system, in order to help business users understand the type of issues that may arise in the course of the relationship, and how quickly and effectively they are likely to be dealt with.

3.2.2.4 Mediation

Pursuant to Article 12, providers of online intermediation services must name in their T&Cs at least two mediators with whom they are willing to engage with in good faith to resolve any disputes that may arise with business users. Providers can choose any mediators, provided they comply with the conditions in Article 12, such as impartiality and independence.

The P2B Regulation provides no further specificity as to what disputes may be mediated.

For mediation pursued under Article 12, the cost is to be shared between the online intermediation service and the business user. Providers are required to pay a reasonable portion of the mediation costs, at the suggestion of the mediator after consideration of relevant factors.

While mediation is a voluntary process, providers are obliged to consider in good faith any requests from business users to engage in mediation to resolve a dispute.

3.2.3 Analysis

The scope of disputes which the P2B Regulation requires platforms to handle through an internal complaints system or through mediation, is wider than the scope of disputes that individuals are required to be able to submit to platforms or take to an out-of-court dispute settlement body under the DSA. This difference in scope of disputes correlates with the different purposes and objectives of the P2B Regulation and the DSA.

The P2B Regulation was created from a perspective of rectifying competition imbalance, rather than addressing the societal issues identified by the DSA. Therefore, the two pieces of legislation will work in combination to address issues experienced by individuals perceived by the European Commission to be detrimental to individual rights and to society; as well as the consequences stemming from an imbalance in bargaining power between platforms and the businesses that rely on them to reach consumers.

Implementation of the P2B Regulation

In January 2021, the Observatory on the Online Platform Economy, set up to support the European Commission in policy making in relation to online platforms, released its study “Monitoring of the implementation of the Platform to Business Regulation”. The study reviewed the terms and conditions of a sample of platforms and search engines, and analysed survey responses from business users, to determine how the P2B Regulation has been implemented since they entered into application in July 2020.

The survey of business users was undertaken in October 2020. Therefore, given the short time in which the P2B Regulation had been in application at that point, the results are not necessarily indicative of the long-term impact of the Regulations. Additionally, at the time the study was conducted, transparency reports were not yet available, for example, regarding the number and types of complaints handled by the internal complaint mechanisms required by Article 11.

The Observatory’s business user survey showed the following:

- More than half of business users did not notice any change in the transparency and clarity of the T&Cs of the main platforms they use. Interestingly, 50% of businesses users surveyed declared using mainly one of the platforms that had introduced recent changes in the T&Cs to comply with the P2B Regulations. This suggests that either the business users had not interacted with the provider in a way in which they may have noticed changes, or that the changes had not been effective enough to result in a perceptible improvement in transparency and clarity.
- On average, 20% to 28% of business users noticed an improvement in transparency relating to their access to data or the possibility to influence the ranking of goods and services on the platform.
- The share of businesses often experiencing problems with the main online platform they use halved since the November 2019 Observatory business survey.
- Among the business users who reported experiencing problems with the main platform they use, most were linked to technical problems, followed by a lack of customer support, sudden changes to pricing and sudden changes to contractual terms.
- The rates of business users using internal complaints handling mechanisms and mediation after experiencing a problem with the platform remained similar between the 2019 and 2020 surveys. The lack of increase may be explained by the fact that some platforms set up their complaint mechanisms or named mediators after the P2B Regulation entered into application in July 2020, and that some users surveyed may be using smaller platforms that are not required to comply with those requirements.
- Between the 2019 and 2020 surveys, the share of businesses that filed an action in court to resolve a problem with a platform significantly reduced, while the number of businesses that used an Ombudsman, arbitration or other dispute resolution method increased.

A more complete understanding of the impacts of the P2B Regulation on the relationships between business users and platforms may be able to be formed once the information on the functioning and effectiveness of internal complaint-handling systems, required under Article 11, is available.

Stakeholder feedback

The European Commission received submissions from Google, Microsoft and Spotify in response to its Inception Impact Assessment for the P2B Regulation.

Google was not supportive of the introduction of regulations to address unfair P2B trading practices, and contested that there was no clear evidence of market failure.

While tensions in business relationships occur, they do not necessarily indicate market failure necessitating an overarching and prescriptive ex ante legislative solution.

Google's submission to P2B Regulation consultation

Google also submitted that a study conducted on the Commission's behalf showed that only about 20 business users out of a community of 1 million developers benefiting from Google Play served as evidence for legislative intervention. Consequently, Google submitted that the policy outcomes the Commission was seeking to achieve could be met via other means, and that market solutions and soft law solutions were already addressing many issues raised in the Inception Impact Assessment.⁹

Microsoft also suggested that a cautious approach should be taken before deciding to intervene in P2B trading practices, noting that many of the practices cited by the Commission were unlikely to warrant intervention on a broad scale and via a one-fits-all solution.¹⁰

The fact that businesses cannot individually negotiate terms with most online platforms, and that most platforms reserve the right to adjust their terms on short notice, is not concerning with appropriate context... New regulation in this area would turn platform size into a liability and drive up costs for all users and harm the EU economy.

New, online-platform specific regulation in the form of notice requirements, appeal guarantees, and other forms of "access rights" would benefit the few platform participants who violate platform terms while harming everyone else.

Microsoft's submission to P2B Regulation consultation

Conversely, Spotify's submission provided examples of the company encountering the types of harmful business practices which the P2B Regulation seeks to address, and supported a targeted legislative approach, including an independent dispute settlement mechanism.¹¹

3.3 Member State regulations

3.3.1 Germany

In 2017, Germany passed a law to address illegal content, [Act to Improve Enforcement of the Law in Social Networks \(Network Enforcement Act, NetzDG\) - Basic Information \(2017\)](#). The provisions of the Act include digital platforms having effective complaints mechanisms, rapid takedown of unlawful content, and bi-annual transparency reports.

The Act applies to telemedia service providers which operate for-profit internet platforms that are designed to enable users to share content with other users or to make such content available to the public. Platforms offering journalistic or editorial content, the responsibility for which lies with the service provider itself, are not covered by the Act.

The Act requires providers to maintain effective and transparent procedures for handling complaints about unlawful content, which ensures:

- removal or blocking of manifestly illegal content within 24hrs, or within 7 days for otherwise unlawful content; and
- that the complainant and the user who posted the content are notified immediately of any decision, while also providing reasons for the decision.

⁹ Google, [Submission to the consultation on fairness in platform-to-business trading practices](#), 2017, accessed 17 March 2021.

¹⁰ Microsoft, [Submission to the consultation on fairness in platform-to-business trading practices](#), 2017, accessed 17 March 2021.

¹¹ Spotify, [Submission to the consultation on fairness in platform-to-business trading practices](#), 2017, accessed 17 March 2021.

It also requires providers that receive more than 100 complaints per year about unlawful content to publish half-yearly reports on the handling of complaints.

Contraventions of these provisions may be sanctioned with regulatory fines of up to 5 million euros.

3.3.2 Austria

On 3 September 2020, the Austrian Government introduced a draft law to combat online hate speech, *Federal Act on measures to protect users on communication platforms (Communication Platforms Act)*. This Act is very similar to Germany's Network Enforcement Act and is applicable to social network providers with more than 100,000 users or with annual revenues exceeding 500,000 euros.

The requirements for providers include:

- Maintaining an effective and transparent procedure for reporting illegal content, including ensuring content is blocked or deleted quickly, and that affected users are informed of the decision. This is the same requirement as in the German NetzDG.
- Provision of a review procedure, whereby the user who reported the content and the user whose content has been blocked or deleted can initiate a review of the decision concerning the blocking or deletion (or absence thereof) by the platform.
- Reporting obligations regarding the handling of reports concerning illegal content.

The draft Act was introduced despite the prior announcement of the DSA, as the consultation and legislative procedure of the EU is a long process, and the Austrian Government saw it necessary to put in place legal measures as soon as possible. This draft Act is intended to be an interim measure until the regulatory deficit has been remedied at the European level.

4. United Kingdom

4.1 Draft Online Safety Bill

On 12 May 2021, the UK government released a draft of its Online Safety Bill. The draft Bill establishes a regulatory framework to address harmful content online, giving effect to the UK government's policy position presented in response to the 2019 Online Harms White Paper.

The draft Online Safety Bill imposes a number of statutory duties on providers of user-to-user services and search engines. While these include duties to operate reporting and redress mechanisms for certain types of complaints, the UK Government Response to the Online Harms White Paper specified that it does not intend to establish an independent resolution mechanism, as outlined below at 4.1.3.1.

The White Paper required the government to decide whether to establish a new regulator or give the additional obligations and powers under the draft Online Safety Bill to an existing regulator. The UK government opted to give additional obligations and powers to the existing UK telecommunications regulator, the Office of Communications (Ofcom).

4.1.1 Who and what it applies to

The regime will apply to providers of online search services and online user-to-user services. User-to-user services are defined in the draft Bill as internet services through which content that is generated by a user of the service, or uploaded to or shared by a user, may be encountered by another user or users.

It applies to:

- Search engines; and
- User-to-user services, including social media services, consumer cloud storage sites, video sharing platforms, online forums, dating services, online instant messaging services, peer-to-peer services, video games that enable interaction with other users online, and online marketplaces.

It does not apply to¹²:

- Email, SMS and MMS services;
- Internal business services where the service is available only to a closed group of employees or authorised persons;
- News publisher content; and
- Low-risk businesses with limited functionality, such as where users can only communicate by posting comments or reviews, or express views only by "liking", rating or voting.

Similar to the EU's approach, the UK's proposed regulatory framework will take a tiered approach. Different expectations will apply to service providers based on the size and scope of their activities. High-risk, high-reach services will be designated as 'Category 1 services', and will correspondingly have increased responsibilities. For example, in addition to taking action in respect of content or activity on their services that is legal but harmful to children, Category 1 services must also take action in respect of content or activity that is legal but harmful to adults.

4.1.2 Key features

4.1.2.1 Duty of care

The duty of care will consist of two parts: the obligations of providers of online search services and online user-to-user services, and the regulator's duties and functions.

Under the statutory duty, providers will have a responsibility to take action to prevent user-generated content or activity on their services causing significant physical or psychological harm to individuals. One of the ways in which providers will fulfil this duty will be by completing regular assessments of the risks associated with their service, and subsequently

¹² UK Draft Online Safety Bill, Schedule 1.

implementing mitigation measures to prevent the identified harms from occurring. The duty is designed to ensure that providers put in place systems and processes that improve user safety. Such systems and processes include user tools, content moderation and recommendation procedures.

All providers in scope of the duty of care will be required to take action against illegal content and activity. All providers will be required to ensure that children are not exposed to *legal* but harmful content.

Definition of harm

The draft Online Safety Bill specifies that online content and activity should be considered harmful where it gives rise to a reasonably foreseeable risk of a significant adverse physical or psychological impact on individuals. The UK Government Response to the White Paper stated that harms to organisations will not fall within the scope of the framework.

The Government Response also specifies that disinformation and misinformation that could cause harm to individuals, such as content which is contrary to public health advice, will be subject to the duty of care. The regulator will have the power to act where disinformation and misinformation presents a significant threat to public safety, public health or national security.

Where there are existing legislative, regulatory and other governmental initiatives in place to combat certain types of harm, these will be outside the scope of the draft Online Safety Bill.

4.1.2.2 Risk assessment and steps to mitigate

As part of the risk assessments required to discharge the duty of care, all providers will be required to consider the risk of harms posed by their service,¹³ including the role the design and operation of the service (including its business model and governance) may have in exacerbating such risks. The steps which providers will be expected to take in mitigating identified risks will be set out by the regulator.

Category 1 Service providers will be required to undertake regular risk assessments to identify legal material that risks harming adult users. This may include content promoting self-harm, hateful content, online abuse that does not meet the threshold of a criminal offence, and content encouraging or promoting eating disorders. Where search and user-to-user services are likely to be accessed by children, those providers will also be required to assess the risk of harm to children due to content on and features of the service.

Category 1 Service providers will also be required to notify the regulator of emerging types of content representing legal but harmful materials that they identify.

This risk assessment requirement is similar to provisions in the EU's DSA, requiring online service providers to assess certain systemic risks that the use and design of their services pose. However, it is not as broad. The UK's risk assessment duties only apply to illegal or harmful content, whereas the EU DSA's proposed systemic risk assessment will address the potential impact on a range of fundamental rights, as well as on a number of matters of public interest.

4.1.2.3 Transparency reporting

Part 3 Chapter 1 of the draft Online Safety Bill sets out transparency reporting requirements of providers. Annual transparency reports will be required to contain information as directed by Ofcom. This may include the prevalence and dissemination of illegal or harmful content on the service; how terms of service and policies are applied; and information about the systems and processes for users to report illegal or harmful content, or other content which is considered to breach the terms of service.

¹³ Sections 7 and 19, UK Draft Online Safety Bill.

4.1.3 User protections

4.1.3.1 Duty to make available reporting and redress mechanisms

Most relevant to the purpose of this report, section 5 of the UK draft Online Safety Bill includes a specific legal duty to have effective and accessible user reporting and redress mechanisms for certain types of content and activity.

As part of this legal duty, all service providers are required to operate their services using systems and processes that allow users or affected persons to easily report content which they consider to be illegal. Services likely to be used by children will also have to operate such systems to allow content considered harmful to children to be easily reported. Category 1 services will be required to operate these systems to allow reporting of content considered harmful to adults.

All providers of user-to-user services will be required to operate a complaints procedure in relation to:

- Content considered to be illegal;
- Non-compliance with a safety duty in Part 2 Chapter 2;
- Non-compliance with the duty in section 12(2) (duties regarding freedom of expression and privacy as set out below at 4.1.3.2); and
- Decisions by providers to warn, suspend, ban or otherwise restrict use of the service due to a user generating, uploading or sharing content which the provider considers to be illegal.

In addition, user-to-user services likely to be accessed by children will be required to operate complaints procedures in relation to:

- Content present on a part of the service able to be accessed by children, which is considered by users and affected persons to be harmful to children;
- Decisions by providers to take down or restrict access to content generated, uploaded or shared by a user because the provider considers that it is harmful to children; and
- Decisions by providers to warn, suspend, ban or otherwise restrict use of the service due to a user generating, uploading or sharing content which the provider considers to be harmful to children.

Category 1 user-to-user services will also be required to operate complaints procedures in relation to:

- Content considered to be harmful to adults;
- Non-compliance with an applicable duty set out in section 12 (protecting freedom of expression and privacy);
- Non-compliance with a duty set out in sections 13 or 14 (protecting content of democratic or journalistic importance, as set out below at 4.1.3.3);
- Decisions by providers to take down or restrict access to content generated, uploaded or shared by a user because the provider considers that it is harmful to adults; and
- Decisions by providers to warn, suspend, ban or otherwise restrict use of the service due to a user generating, uploading or sharing content which the provider considers to be harmful to adults.

In addition, as discussed below at 4.1.3.3, Category 1 user-to-user services have an additional duty to have a dedicated and expedited complaints procedure available for complaints about journalistic content.

This dedicated and expedited complaint procedure must ensure that actions taken are swiftly reversed, or content swiftly reinstated, if the complaint is upheld.

Providers of search services also have redress requirements in relation to the following complaints:

- Content the provider considers to be illegal, or harmful to children where the services is likely to be accessed by children;
- Non-compliance with Part 2 Chapter 3 safety duties;
- Non-compliance with the duty about rights to freedom of expression and privacy in section 23; and
- Complaints by an interested person about steps taken by the provider to comply with safety duties about illegal content under sections 21 or 22, which result in content relating to that interested person no longer appearing or being given a lower priority in search results.

All service providers have a duty to make the policies and procedures that govern the handling and resolution of the types of complaints set out above publicly available and easily accessible (including to children).

All complaints procedures must provide for appropriate action to be taken by the provider in response to complaints, be easy to access and use, and be transparent.

The draft Bill does not specify what form ‘appropriate action’ must take. Notably, the UK Government Response to the White Paper made clear that it will not mandate specific forms of redress and it does not intend to establish an independent resolution mechanism, such as an ombudsman or certified alternative dispute resolution scheme. One justification offered for this is that such mechanisms are relatively untested in relation to non-financial harm, and the central issues in the disputes covered by the White Paper are user safety and users’ rights.¹⁴ Additionally:

Establishing an independent mechanism for resolving disputes would not align with our overarching objective to ensure companies take more responsibility for their users’ safety, and to improve users’ trust in their processes. It could disincentivise cultural change within companies, and encourage companies to ‘offload’ difficult content decisions externally.

Online Harms White Paper Government Response

The Government Response sets out that forms of redress companies may offer include:

- content removal;
- sanctions against offending users;
- reversal of wrongful content removal or sanctions;
- mediation; or
- changes to company processes and policies.

4.1.3.2 Freedom of expression and privacy

All service providers within scope of the framework will be required to consider the impact on, and include safeguards for, users’ rights when designing and implementing systems and processes intended to reduce harms to users.

Specifically, all providers will have a duty to have regard to the importance of protecting the rights of users to freedom of expression within the law, and of protecting users from unwarranted infringements of privacy, when deciding on and implementing safety policies and procedures.¹⁵ “Safety policies and procedures” includes any of the reporting and redress duties set out above at 4.1.3.1.

Providers of Category 1 user-to-user services will also have a duty to carry out an impact assessment of proposed and adopted safety policies and procedures on protection of freedom of expression and from unwarranted infringements of privacy. Category 1 services will be required to specify in their T&Cs the steps taken in response to an impact assessment to better protect users’ rights.

This element of the UK’s proposed framework is similar to the EU DSA’s provisions requiring an assessment of systemic risks posed by online services, as one of the specific systemic risks is the impact that services have on the fundamental human right to free expression. Incorporating consideration of the impact on individuals’ rights into design of services would reduce instances in which it is appropriate or necessary for users to resort to dispute resolution.

This approach recognises the importance of high risk, high reach platforms as public forums where people can engage in robust debate online. Companies will not be able to arbitrarily remove controversial viewpoints and users will be able to seek redress if they feel content has been removed unfairly. When combined with transparency requirements, will also increase understanding about what content is taken down and why. In this way, regulation will promote and safeguard pluralism online, while ensuring companies can be held to account for their commitments to uphold freedom of expression.

Online Harms White Paper Government Response

¹⁴ Paragraphs 4.32-4.33, UK Government Response to the Online Harms White Paper.

¹⁵ Sections 12 and 23 UK Draft Online Safety Bill.

4.1.3.3 Journalistic content and content of democratic importance

In addition to the above duties, Category 1 user-to-user services have additional duties in relation to journalistic content and content of democratic importance, consisting:

- A duty to operate the service using systems and processes designed to ensure that the importance of the free expression of content of democratic importance and of journalistic content is taken into account when making decisions about how to treat such content (including decisions about whether to take it down or restrict access to it), and decisions about whether to take action (by warning, suspending, banning or otherwise restricting use) against a user who has generated, uploaded or shared such content;
- A duty to apply the above systems and processes consistently across the diversity of political opinion; and
- A duty to specify in T&Cs the policies and processes designed to take into account the free expression of journalistic content and content of democratic importance, and how these will be applied to decisions to treat that content or take action against users.¹⁶

The draft Bill specifies that content will be considered to be “of democratic importance” if it is news publisher content or regulated content, and it is or appears to be specifically intended to contribute to democratic political debate in the UK. “Regulated content” is content not excluded from the Bill’s framework under Schedule 1, as set out above at 4.1.1.

Category 1 services also have an additional duty to operate a dedicated and expedited complaints procedure through which users can submit complaints about decisions by providers to:

- Take action against a user because of content generated, uploaded or shared by the user, which the user considers to be journalistic content; or
- Take down or restrict access to content that the user who generated, uploaded, shared or created the content considers to be journalistic.¹⁷

The policies and processes for handling complaints in relation to journalistic content must be set out in the T&Cs, along with the methods through which content is identified as journalistic content. These T&Cs must be clear, accessible, and applied consistently.

4.1.3.4 Super-complaints

The regulatory framework includes provisions that ensures that there is an avenue for “eligible entities” to alert the regulator to their concerns about systemic issues. Such complaints are labelled as “super-complaints”.

The draft Online Safety Bill states that the criteria for eligibility of entities will be specified in regulations. The Government Response to the White Paper suggests this will include organisations representing users or those who are affected by harmful content and activity online.

Super-complaints will be accepted by the regulator where features of a service or conduct of providers appears to, or presents a material risk of:

- Causing significant harm to users or members of the public;
- significantly adversely affecting the rights to freedom of expression within the law of users or members of the public;
- causing significant unwarranted infringements of privacy; or
- Otherwise having a significant adverse impact on users or members of the public.

Super-complaints will need to focus on the systems and processes that companies have in place, rather than any specific content issues. They will also need to focus on issues occurring across multiple in-scope services, as organisations can raise concerns about a single company’s conduct through Ofcom’s enforcement complaints processes.

Online Harms White Paper Government Response

This is similar to the EU’s provisions on trusted flaggers in the proposed Digital Services Act.

¹⁶ Sections 13 and 14 UK Draft Online Safety Bill.

¹⁷ Subsections 14(3) and (4) UK Draft Online Safety Bill.

4.1.4 Role of the regulator

The White Paper required the UK government to decide whether to establish a new regulator or give the additional obligations and powers that will be introduced under the Online Safety Bill to an existing regulator. The Government Response named the existing UK telecommunications regulator, Ofcom, as the appropriate body.

The cost to the regulator of implementing the online harms scheme will be offset by industry fees. Providers that exceed a global annual revenue threshold will be required to notify the regulator and pay an annual fee.¹⁸

The government recognises the need to balance effective enforcement with protecting the attractiveness of the UK as a tech sector, and also with users' rights. The regulator will strongly encourage compliance with the regime in the first instance and provide clear grounds for any intervention and escalation. The focus will be on ensuring that companies have compliant systems and processes in place, rather than on specific pieces of content.

Online Harms White Paper Government Response

The regulator's enforcement powers will include¹⁹:

- Power to investigate, issue directions and notices of non-compliance.
- Power to issue fines up to £18m or 10% of annual global turnover, whichever is higher.
- Power to require information for the purpose of exercising online safety functions. Failure to comply with an information notice can result in criminal penalties.²⁰ Ofcom can also require providers to name a senior manager, and failure to comply with an information request can result in criminal liability for the named senior manager.²¹ Note that there are additional provisions about the liability of controlling individuals, entities and fellow subsidiary entities.²²
- Business Disruption Measures²³:
 - The regulator will be required to obtain a court order for Business Disruption Measures.
 - The regulator will have the power to take measures that make it less commercially viable for a non-compliant provider to provide services to UK users.
 - The regulator will have the power to require providers to withdraw access to key services. If providers do not comply, the regulator will be able to enforce through a court order.
 - The regulator will have the power to take measures that block a non-compliant provider's services from being accessible in the UK, by requiring the withdrawal of services by key internet infrastructure providers (e.g. browsers, web-hosting companies, app stores, online security providers or Internet Service Providers). This approach is technology neutral to encompass future changes to how the architecture of the internet functions.

The regulator will also be able to draft codes of practice outlining how service providers can fulfil their duties, which will assist in providing clarity around their obligations.²⁴

Notably, the regulator will not investigate or arbitrate individual cases. The regulatory framework will not create new avenues for individuals to bring civil action against platforms. Rather, the statutory duty of care is intended to reduce some of the difficulties individuals face in obtaining remedies in court for negligence or breach of contract. It is expected to increase the effectiveness of individuals' existing legal remedies, for example by clarifying that a duty exists, and by establishing a causal link between the activities of platforms and harm caused to individuals.²⁵

4.1.5 Analysis

The UK's Online Safety Bill does not appear to be as broad in scope as the EU's proposed DSA. For example, it does not specify that platforms will be subject to online advertising transparency requirements or that they will be required to

¹⁸ Sections 52 and 53 UK Draft Online Safety Bill.

¹⁹ Part 4 Chapter 6 UK Draft Online Safety Bill.

²⁰ Section 72 UK Draft Online Safety Bill.

²¹ Section 73 UK Draft Online Safety Bill.

²² Sections 118-121 UK Draft Online Safety Bill.

²³ Sections 91-94 UK Draft Online Safety Bill.

²⁴ Part 2 Chapter 5 UK Draft Online Safety Bill.

²⁵ [Online Harms White Paper: Full Government Response to the consultation](#), 2020, at paragraph 3.29.

provide a statement of reasons for decisions relating to a user's use of their services. The UK's proposed framework focuses specifically on "harm" arising from content encountered on platforms, whereas the EU's approach also takes into account impacts arising from the business structure of platforms.

The White Paper provides some limited justification for the implementation of statutory duties of care, as opposed to standards or other requirements. Beyond the benefits to individuals in pursuing existing civil courses of action outlined above at 4.1.4, the Paper states:

There is currently a patchwork of regulation and voluntary initiatives aimed at addressing [online content or activity that harms individual users or threatens our way of life in the UK], but these have not gone far or fast enough to keep UK users safe online.

Online Harms White Paper

As discussed above at 4.1.3.1, the UK Government Response to the White Paper indicated that an independent resolution mechanism, such as an Ombudsman or certified alternative dispute resolution scheme, would not be a requirement because such mechanisms are relatively untested in areas of non-financial harm, and because it would not be consistent with the systems and processes approach.

However, if platforms were required to engage in good faith in out-of-court dispute settlement, and are required to bear some or all of the costs, then it would incentivise platforms to design processes and systems that resolve disputes before they escalate to the level of requiring external dispute resolution. This is consistent with a systems and processes approach.

Further, the Government Response suggests mediation as a recourse avenue, which does not accord with the systems and processes approach. This approach is intended to cause cultural change in the design of services to prioritise the safety and well-being of users. Mediation is less likely to encourage cultural change because it is conducted in private, and the mediator has no investigative powers or ability to look into systemic issues.²⁶

The Department will continue to engage with the UK to gain further understanding around its approach to external dispute resolution and how it relates to the systems and processes method.

²⁶ Federal Court of Australia, [Mediation](#), Federal Court of Australia website, n.d., accessed 16 March 2021.

5. North America

5.1 United States

The United States has taken a relatively hands off approach to the regulation of digital platforms, based on the principle of a free and open internet and in pursuit of protection of the First Amendment right to free speech. This approach has allowed innovation in the technology sector, but it has also resulted in a concentration of power amongst a relatively small number of private companies. These companies have developed their own policies in relation to content moderation and dispute resolution, and their power compared to both business users and consumers means that they are able to impose these policies unilaterally. For example, as at November 2018, the vast majority of America's largest companies, including Amazon, Facebook (and Instagram), and Alphabet, employed mandatory arbitration clauses in their terms of use.²⁷

Arbitration clauses can require consumers to submit any disputes that may arise between them and the provider to binding arbitration. These are usually included in unilaterally determined click-wrap agreements to which users must agree in order to use a service.

While arbitration does have benefits as a form of dispute resolution, such as efficiency, informality and lower costs,²⁸ many of these benefits accrue in favour of the digital platform where arbitration is unilaterally imposed on the user. Providers are able to stipulate who will administer the proceedings, according to what rules, and in which jurisdiction arbitration must occur. Furthermore, arbitration is conducted in private, with outcomes not typically made public. It therefore does not serve to address systemic risks or increase transparency and accountability of platforms.

There have, however, been reform proposals and processes initiated with the intent of reducing the systemic risks imposed by digital platforms, and to increase their accountability. These have included:

- Reducing bargaining power by breaking up tech monopolies through antitrust proceedings;
- Bans on vertical integration; and
- Calls to reform Section 230 of the US *Communications Decency Act 1996*, which protects providers from liability both for content posted by users and for removing certain types of content contrary to the right to free speech.

There are also recent examples of proposals to import elements from regulations in international jurisdictions that employ alternative tactics to address issues stemming from the concentration of bargaining power in large digital platforms. One such proposal, introduced to Congress in June 2020, has similar aspects to the UK Online Harms White Paper and EU legislation.²⁹ The Platform Accountability and Consumer Transparency Act (PACT Act) proposes the following requirements:

- Minimum standards for Acceptable Use Policies (AUP);
- An easily accessible complaints system; and
- An intermediary liability standard, through an amendment to Section 230 preventing platforms from relying on the protections where they fail to remove illegal content or activity on their platform within 24 hours of acquiring knowledge of its existence.

The proposed minimum AUP standards include informing users of the types of content allowed on the service; explaining the steps providers take to ensure content complies with the AUP; and explaining the means by which users can notify the provider of policy-violating content or illegal content or activity. Such notification mechanisms must include a live company representative available to take telephone complaints during business hours; an email address or relevant complaint intake mechanisms; and a complaint-handling system. It is also proposed that providers will produce quarterly transparency reports.

The complaint-handling system referred to above is proposed to deal with good faith user complaints regarding potentially policy-violating content; illegal content or activity; or decisions by the provider to remove content. The PACT

²⁷ Imre Stephen Szalai, 'The Prevalence of Consumer Arbitration Agreements by America's Top Companies', *UC Davis Law Review Online*, 2019, 52:233.

²⁸ Kelsey L Swain, '[Alternative Dispute Resolution and Social Media: How Mandatory Arbitration Clauses Impact Social Networking](#)', *Arbitration Law Review: Yearbook on Arbitration and Mediation*, 2020, 5:356-370, p 365.

²⁹ [Bill S.4066](#), 116th Congress (2019-2020).

Act would require providers to stop or remove illegal content or activity within 24 hours, and process complaints about otherwise potentially policy-violating material within 14 days.

Interestingly, the Act would require the provider to notify users of decisions to remove content whether based on a user complaint or on a moderation decision of the provider. However, the provider would only be required to allow the user who posted the content to appeal the decision where it was based on a user complaint.

The PACT Act does not propose any external dispute resolution processes.

The bill has been referred to the Committee on Commerce, Science, and Transportation for consideration.

5.2 Canada

Canada has proposed a multi-pronged approach to the regulation of digital platforms, with the intent of addressing the current 'imbalance that favours web giants' over business users and consumers.³⁰ The approach involves:

- Bill S-225, introduced on 17 February 2021, requires platforms to remunerate for journalistic content shared on their platform, in a manner similar to the Australian Government's News Media Bargaining Code;
- Bill C-10, which is currently being considered before the Standing Committee on Canadian Heritage, amends the Broadcasting Act to include online undertakings that deliver audio and audio-visual content as a class of broadcasters subject to the Act. The Bill provides new powers to the Telecommunications Commission to regulate online services, aimed at levelling the playing field between traditional and online broadcasting services.
- The Digital Charter Implementation Bill C-11, which establishes requirements to increase transparency around the use of individuals' data; and
- Planned legislation to deal with illegal content posted on platforms.

Relevantly, the Digital Charter Implementation Bill 2020 imposes requirements on companies to provide information to gain consent for the use of data in plain language; establishes a right to withdraw consent to data collection and have data deleted; establishes a right for users to direct and transfer data from one organisation or entity to another; and imposes transparency requirements on the use of automated systems for the making of significant decisions or predictions about users. The Bill would also give users the right to an explanation of a prediction or decision made by such systems.

The Bill gives powers and responsibilities to the existing Privacy Commissioner to ensure compliance. To hear appeals of certain decisions made by the Commissioner, the Bill establishes the Personal Information and Data Protection Tribunal.

Bill C-11 requires organisations to designate one or more individuals to deal with matters related to its obligations under the Bill, and provide contact details. This requirement is in line with Articles 10 and 11 in the EU's Platform-to-Business Regulations, which require designation of a single point of contact and legal representative.

The Bill also proposes that individuals may request in writing that an organisation informs them of whether it holds any personal information about them, how it uses the information and whether it has disclosed the information. If an organisation refuses a request, it must inform the individual of the reasons for refusal and of any recourse available to them under the Bill.

Recourse options include:

- An individual may make a complaint, or a request for information, to an organisation with respect to its compliance with Part 1 of the Bill, which encompasses all measures outlined above;
- An individual may file a complaint with the Commissioner against an organisation for contravention of Part 1. The Commissioner may also initiate a complaint. If the matter is not resolved or discontinued after investigation, the Commissioner may conduct an inquiry into the matter.

Provided a complaint complies with procedural requirements and that the Commissioner is of the opinion that the complainant has first exhausted grievance or review procedures otherwise reasonably available to it, the Commissioner must investigate the complaint.

³⁰ Standing Committee on Canadian Heritage, [Meeting of 29 January 2021](#).

Under the Bill, if a complaint is not the subject of an inquiry, the Commissioner may attempt to resolve the complaint by means of an alternative dispute resolution method such as mediation or conciliation.

The provisions of Bill C-11 are limited in scope compared to the legislation proposed and enacted by the EU and UK. It creates mechanisms to resolve disputes only relating to the use of personal data. Further dispute resolution mechanisms may be included in planned legislation to deal with harmful content, which is expected to be introduced in early 2021.

5.3 Mexico

In February 2021, the governing party of Mexico presented a proposed set of amendments to the Telecommunications and Broadcasting Law, for public comment. The proposal is aimed at regulating social media providers, following the de-platforming of international political figures on social media platforms such as Twitter. The proposal states that the object of regulation would be the protection of human rights, principally freedom of expression.

The scope of the proposed regulation is limited to “social networks”, rather than “online intermediary services” as in the EU’s DSA, and would only apply to platforms with over one million users in Mexico.

The proposed amendments would require platforms to have an internal appeals mechanism in place for decisions to block or cancel user accounts. Platforms would have 24 hours to affirm or revoke the decision, and this must be done by humans. If users wish to challenge the decision to affirm or revoke, they can then appeal to the existing federal telecommunications regulator. Failure to comply with the proposed regulatory duties would open platforms to significant financial penalties.

This proposal is intended to provide robust protections for freedom of expression; however, it may do so at the expense of platforms’ ability to take down content they believe to be harmful. The balance between protecting freedom of expression and protecting against exposure to harm online may be tipped too far in favour of the former. Furthermore, the burden of establishing human committees capable of taking decisions on any appealed blocking or cancellation within 24 hours would be great.

6. New Zealand and Singapore

6.1 New Zealand

The New Zealand government has intervened relatively little in the regulation of digital platforms. The most relevant government action relating to digital platforms is the Christchurch Call to Action – a set of voluntary commitments for governments and online service providers, aimed at eliminating terrorist and violent extremist content online. The adoption of the Christchurch Call was led by New Zealand and France following the Christchurch attacks in 2019, and is supported by Australia. Online service provider supporters include Facebook, Google, Amazon, Twitter and Microsoft.

Relevantly, the Call asks providers to commit to:

- Providing greater transparency in the setting of community standards or terms of service, including outlining and publishing the consequences of sharing violating material, and describing the policies and procedures for detecting and removing such content;
- Enforcing community standards or terms of service in a manner consistent with human rights and fundamental freedoms, including by providing an efficient complaints and appeals process for those wishing to contest the removal of their content or a decision to decline the upload of their content;
- Implementing regular and transparent public reporting on terrorist and violent extremist content detected and removed from the platform; and
- Reviewing the operation of algorithms and other processes that may drive users towards or amplify terrorist and violent extremist content. This may include building appropriate mechanisms for reporting content.

It is unclear whether the Christchurch Call has had a tangible effect on the business practices of platforms. There are elements of these voluntary platform commitments that the EU, Australia, and the UK have considered necessary to enshrine in legislation,³¹ indicating that the voluntary approach for this type of content may not be sufficiently effective to prevent harm occurring online.

6.2 Singapore

Internet Service Providers (ISPs) and Internet Content Providers (ICPs) in Singapore are regulated through the Broadcasting (Class Licence) Notification, under the Broadcasting Act. They are required to abide by the conditions stated in the Internet Class Licence and ensure that content offered complies with the Internet Code of Practice. Neither the Internet Class Licence nor the Internet Code of Practice include requirements for appeal or redress avenues for users.

The Singaporean government takes a light-touch approach towards over-the-top services, such as Facebook and WhatsApp, which do not need a licence to offer services in Singapore.³²

Facebook is, however, subject to the Protection from Online Falsehoods and Manipulation Act, which came into force in October 2019.³³ This legislation allows the Singaporean government to issue correction notices, or directions to cease communication, to people who have communicated false statements of fact that are considered to be detrimental to certain public interests, including diminishing public confidence in the general governance of Singapore. Correction directions can also be issued to internet intermediaries, which would then be required to publish a correction notice. The only redress mechanism built into this legislation is the ability to apply to the minister who issued the direction, and subsequently to the High Court, to vary or cancel any directions.

³¹ For example, in the EU DSA, Australia's Online Safety Bill 2021, and the UK's Online Harms White Paper.

³² Medha Basu, '[Inside Singapore's tech regulation efforts](#)', *GovInsider*, 8 April 2019, accessed 9 March 2021.

³³ BBC, '[Facebook expresses 'deep concern' after Singapore orders page block](#)', *BBC News*, 19 February 2020, accessed 9 March 2021.

7. Other Standards and Guidelines

7.1 Internet Governance Forum

The Internet Governance Forum (IGF) is a global, multi-stakeholder governance group for policy dialogue on issues of internet governance, which was convened by the Secretary-General of the United Nations in 2006. Its sub-committee, the Dynamic Coalition on Platform Responsibility (DCPR), formed an ad hoc working group at the 2019 IGF on the implementation of the right to an effective remedy, enshrined in article 2.3 of the International Covenant on Civil and Political Rights, in the context of online platforms. The Working Group published the outcome document '[Best Practices on Platforms' Implementation of the Right to an Effective Remedy.](#)'

The best practices were identified by merging solutions that effectively balance the protection of users' rights with considerations of the viability of digital platforms' business models. The document includes both a set of recommendations for platforms to implement and maintain alternative appeals mechanisms, and an analysis of existing legal agreements and Terms of Use between platforms and users.

The Working Group's recommendations include:

- Where a platform restricts the type of content deemed acceptable, its terms of service shall set out in a clear and detailed manner the type of content considered acceptable. In so doing, platforms shall consider their responsibility to respect human rights, including freedom of expression.
- Platforms should provide meaningful notice of any change to their T&Cs at least 30 days before the changes go into effect.
- Platforms shall offer notice mechanisms to report behaviours that violate the T&Cs, such as flagging content and/or by filling in a form.
- Platform users shall have the right to initiate litigation and take part in class actions in their own jurisdiction, and such rights shall always be available where the platform targets a jurisdiction such as by using the local language, currency or country code domain name.
- Platforms shall notify affected individuals prior to the adoption of any adverse measures. Notice shall include the specific grounds on which such measures were taken. Platforms should allow the individual to contest a notified measure prior to adoption, and shall always allow them to contest the measure after adoption.
- Platforms should have mechanisms in place on their website to allow users to resolve disputes arising between them and the platform in relation to their platform activity.
- Platforms that receive requests for content removal shall only implement deletion after an internal human review. Users shall always have the possibility to challenge automated deletion, and to have such deletion reviewed by a human.
- Platforms shall provide an alternative dispute resolution mechanism, designed in a flexible way based on generally accepted procedural rules. This mechanism should not serve as a pre-requisite to or substitute for litigation. Platform users shall always have a meaningful opportunity to opt out.
- There should be a reasonable time limit for the resolution of disputes, such as 30 days, set by platforms.
- Platforms should have in place additional mechanisms to complement those set out above, in fulfilment of their corporate social responsibility to respect human rights and to have in place processes to enable remediation of any adverse effects on human rights that they cause.

It is clear that many of these recommendations have been taken on board by the European Union in both the P2B Regulation and the proposed Digital Services Act. For example, as outlined in 3.2.2.1 above, the P2B Regulation includes comprehensive minimum standards for T&Cs, mirroring a number of the above recommendations such as a notice period for changes to T&Cs, explanations of any restrictions applicable to users, notification prior to the adoption of adverse measures against users, internal dispute resolution processes, and an alternative dispute resolution mechanism in the form of mediation.

7.2 Santa Clara Principles

In February 2018, the Santa Clara Principles on Transparency and Accountability in Content Moderation were created by a small group of organisations, academics, and advocates at the first Content Moderation at Scale conference in Santa Clara, California. The principles provide a set of baseline standards or initial steps that companies engaged in content

moderation should take to provide meaningful due process to impacted speakers and better ensure that the enforcement of their content guidelines is fair, unbiased, proportional, and respectful of users' rights. The principles include:

- **Numbers** - Companies should publish the numbers of posts removed and accounts permanently or temporarily suspended due to violations of their content guidelines. This data should be accessible through regular reporting, ideally quarterly.
- **Notice** - Companies should provide notice to each user whose content is taken down or account is suspended about the reason for the removal or suspension. Companies should also provide detailed guidance about what content is allowed on their platform, the guidelines used by reviewers, and an explanation of how automated detection is used to detect violating content.
- **Appeal** - Companies should provide a meaningful opportunity for timely appeal of any content removal or account suspension. Minimum standards for meaningful appeal include human review, an opportunity to present additional information, notification of the result of review and a statement of the reasoning sufficient to allow the user to understand the decision. An independent external review process may be an important redress avenue in the longer term.

A large number of digital platforms have publicly endorsed the principles, including Facebook, Twitter, Instagram and YouTube.³⁴ Some companies have implemented the principles in part, and Reddit has incorporated the principles in full in its policies.³⁵

These principles are consistent with what was recommended by the DCPR at the 2019 IGF, and with what has been implemented and proposed by the EU and, to a lesser extent, the UK.

7.3 OECD's Recommendation on Consumer Protection in e-Commerce

In 2016, the Organisation for Economic Co-operation and Development (OECD) published a recommendation on the protection of consumers in the context of e-commerce. Despite the developments in e-commerce that have occurred in the ensuing five years, the OECD's Recommendation remains relevant and is in line with the principles and recommendations outlined in the sections above. It also demonstrates that the need for dispute resolution mechanisms was evident in 2016 and, considering that online commerce has continued to increase in prevalence since that time,³⁶ suggests that the need is now greater.

The Recommendation applies to business-to-consumer electronic commerce, including commercial practices through which businesses facilitate consumer-to-consumer transactions. Regarding dispute resolution and redress, the Recommendation provides the following:

Consumers should be provided with meaningful access to fair, easy-to-use, transparent and effective mechanisms to resolve domestic and cross-border e-commerce disputes in a timely manner and obtain redress, as appropriate, without incurring unnecessary cost or burden. These should include out-of-court mechanisms, such as internal complaints handling and alternative dispute resolution.

OECD Recommendation on Consumer Protection in e-Commerce

³⁴ Gennie Gebhart, 'Who Has Your Back? Censorship Edition 2019', *Electronic Frontier Foundation*, 2019, accessed 4 May 2021.

³⁵ <https://santaclaraprinciples.org/cfp/>, Santa Clara Principles website, March 2020, accessed 4 May 2021.

³⁶ Tugba Sabanoglu, *Global retail e-commerce sales 2014-2023*, Statista website, 2020, accessed 11 March 2021.

s47C - deliberative processes



s47C - deliberative processes

s47C - deliberative processes





Australian Government

Department of Infrastructure, Transport,
Regional Development and Communications

Attachment D – Details of Existing External Escalation Mechanics

This attachment provides an outline of the range of EDR systems currently available, and the powers and remit of each.

Australian Small Business and Family Enterprise Ombudsman

The Australian Small Business and Family Enterprise Ombudsman (ASBFEO) is a government-run Ombudsman that provides assistance and advocacy functions to Australian small businesses and family enterprises (SBFEs). It was established by, and is governed by the *Australian Small Business and Family Enterprise Ombudsman Act 2015* ('ASBFEO Act') and the *Australian Small Business and Family Enterprise Ombudsman (Consequential and Transitional Provisions) Act 2015*. Responsibility for this legislation sits with the Treasury.

The ASBFEO's assistance function consists of support in the management of the dispute resolution process. Through its advocacy function, the ASBFEO conducts inquiries and research; works with other arms of government; contributes to other inquiries; and promotes good business practice.

Assistance Function

In discharging its assistance function, the ASBFEO has the power to respond to requests for assistance in relation to "relevant actions". Section 7 of the ASBFEO Act defines "actions" to include activities, projects, making a decision or recommendation, or an alteration of, failure or refusal to do any of those things. "Relevant action" is defined in section 65, and includes action by an entity that affects, or may affect, a SBFE in the course of trade or commerce between Australia and places outside Australia, or within Australia. It is therefore possible that ASBFEO would have authority to assist with any in-scope issue, where the "action" of an entity affects a small business in trade or commerce.

"Relevant action" also includes conduct affecting a SBFE that may be in contravention of Part IV of the *Competition and Consumer Act 2010*, which includes misuse of market power.¹ For these types of relevant actions, the ASBFEO has additional powers to assist with the preparation of arguments and evidence in relation to costs orders under that Act.

The ASBFEO has the power to make recommendations about how a dispute about relevant actions may be managed, including recommending that an ADR process be used.² ADR processes are defined in section 4 of the ASBFEO Act to include:

- Conferencing
- Mediation
- Neutral evaluation

¹ *Competition and Consumer Act 2010* (Cth) s 46.

² ASBFEO Act s 71.

- Case appraisal
- Conciliation
- Prescribed procedures or services

The definition explicitly excludes arbitration and court procedures or services.

In practice, the ASBFEO Assistance Team firstly provides information on how to resolve disputes and facilitates discussions between disputing parties. This requires the ASBFEO to locate a platform contact. If the dispute is not resolved at this stage, the ASBFEO can refer SMFEs to an appropriate ADR process.³ Where the ASBFEO makes such a recommendation, the ADR process must not be conducted by the ASBFEO.⁴

Where an entity who is party to a dispute refuses to engage in or withdraws from an ADR process that has been recommended by the ASBFEO, the ASBFEO may publicise that fact.⁵

In pursuing requests for assistance, the ASBFEO may exercise its information-gathering powers. These powers include:

- making inquiries to assist in deciding whether it has authority to deal with a request;
- deciding whether the request would be better dealt with by another agency or whether it will recommend ADR processes;⁶ and
- issuing notices to provide information relevant to an inquiry set out in section 75. Failure to comply with a notice carries a penalty of 30 penalty units, amounting to \$6660 at date of writing.

Analysis

The ASBFEO's assistance function does offer a pathway for small businesses to externally escalate an issue, provided it falls within the ASBFEO's remit detailed above. However, its powers to assist in resolving a dispute are limited. The first step of the ASBFEO's process – facilitating discussion – is reliant upon platforms offering a contact point, or the ASBFEO having previously cultivated a relationship with the platform. The ASBFEO has indicated that this can be time consuming, and depends largely upon the good will of platforms.⁷ **s47C - deliberative processes**

The second step in the process is referral to external ADR. In comparison with the state small business bodies, for example, where ADR is performed by the body itself, this step adds an extra layer to the process and may require the business to retell their story to multiple bodies. As a consequence, it may make small businesses less satisfied with the services provided by ASBFEO.

In addition, the ASBFEO can only refer small businesses to non-binding forms of ADR. Non-binding ADR may not present an effective resolution option for individual issues because platforms may not face consequences for failing to come to a resolution or for not adhering to an agreed resolution. Non-binding ADR is also unlikely to have a strong deterrent effect on platforms.

s47C - deliberative processes

³ [How we help | Australian Small Business and Family Enterprise Ombudsman \(asbfeo.gov.au\)](#)

⁴ ASBFEO Act s 73.

⁵ ASBFEO Act s 74.

⁶ ASBFEO Act s 75.

⁷ EDR Scheme Advisory Panel Meeting 1.

Australian Communications and Media Authority (ACMA)

ACMA is the federal government regulator for communications and media. It is an independent Commonwealth statutory authority, established by the *Australian Communications and Media Authority Act 2005* ('ACMA Act'). Its purpose is to maximise the economic and social benefits of communications and media for Australia.

ACMA has the following functions:

- Telecommunications functions – regulation of the telecommunications industry in accordance with the Telecommunications Act 1997, and other functions as conferred by various legislation including the Spam Act 2003 ('Spam Act');
- Spectrum management;
- Broadcasting, content and datacasting functions – regulation of broadcasting services in accordance with the Broadcasting Services Act 1992; and
- Any functions conferred on it by any other law.

Of these, the only ACMA functions that relate to an in-scope issue are those conferred under the Spam Act.

Spam

The Spam Act prohibits the sending of unsolicited commercial electronic messages. Other requirements for commercial electronic messages set out in the Spam Act are that it must include information about who authorised the message, and must include a functional unsubscribe facility.

Electronic message includes messages sent using an internet carriage service, to an electronic address in connection with an email account; an instant messaging account; a telephone account; or a similar account.⁸

A message can be commercial in nature regardless of whether the goods or services or opportunity it offers actually exists.⁹ This means that scam advertisements that meet the criteria may also constitute spam.

Users can make a complaint about spam to ACMA, following which ACMA may contact the sender about their responsibilities under the Spam Act and may investigate serious or ongoing issues. People can also report spam to ACMA, which does not register as a complaint but allows ACMA to identify spam trends and potential compliance issues.

Breaches of the provisions which prohibit sending unsolicited electronic commercial messages; require information about the sender be provided; and require unsubscribe functions be made available are civil penalty provisions carrying pecuniary penalties. ACMA also has a range of enforcement options open to it for breaches of civil penalty provisions. These include injunctions, enforceable undertakings, and formal warnings.¹⁰

It is important to note that the obligations and penalties in the Spam Act are directed at the sender of spam messages, rather than the platform on which they are sent. Therefore, investigations or enforcement action would be against the user who sent the message.

Analysis

ACMA does provide a pathway for external escalation of "spam" in the narrow legal sense under the Spam Act. Users of instant messaging platforms or "similar accounts", which could potentially include social media accounts in general, who receive unsolicited electronic commercial messages can make a complaint to ACMA. However, this definition of spam does not necessarily capture the entirety of a layperson's understanding of what constitutes spam. In its Report,

⁸ Spam Act 2003 s 5.

⁹ Spam Act 2003 s 6.

¹⁰ Spam Act 2003 pts 4–7.

Accenture defined spam to include “content that is unsolicited, annoying and usually posted or sent in bulk”. The breadth of the issue defined as such would therefore not fall fully within ACMA’s remit.

In addition, ACMA’s powers to respond to the complaint are limited by the need to identify the sender. This may be especially difficult where the spam is sent via social media. This being said, ACMA does have information-gathering powers relating to commercial electronic messages. These are contained in the *Telecommunications Act 1997*, and allow ACMA to obtain information and documents from carriers, service providers or other persons, where it is relevant to the discharge of its telecommunications functions. Section 522(2) of the *Telecommunications Act* specifies that “person” includes a body corporate.

s47C - deliberative processes

Australian Cyber Security Centre (ACSC)

The ACSC is based within the Australian Signals Directorate, and provides advice and information about how Australian individuals and businesses can protect themselves online.

The ACSC receives reports of cybercrime through its ReportCyber function. However, it has no power to deal with complaints itself and refers them to the appropriate police jurisdiction for assessment. It is also unable to advise on the progress of any reports made to it.

Hacking, fake accounts and scams are likely the only in-scope issues that have the potential to amount to cybercrimes, such as identity theft or online fraud.

State Small Business Bodies

Some states have independent statutory bodies that offer relevant dispute resolution services to small businesses. These include:

- Victorian Small Business Commission
- New South Wales Small Business Commissioner
- Western Australia Small Business Development Corporation
- South Australian Office of the Small Business Commissioner

The Office of the Queensland Small Business Commissioner was established under the *COVID-19 Emergency Response Act 2020* (Qld), and is now in the process of transitioning to a permanent service. While the QSBC currently only provides dispute resolution assistance for leasing disputes, its powers may change as it transitions to a permanent service.

The functions and powers of each State body are different and defined by the body’s establishing legislation. Below is an overview of the functions and powers of the Victorian Small Business Commission and NSW Small Business Commissioner.

Victorian Small Business Commission

The Victorian Small Business Commission was established by the *Small Business Commission Act 2017* (Vic) (‘VSBC Act’), with its functions and powers set out in section 5 of the legislation.

The Commission can receive and investigate complaints by small business regarding unfair market practices or commercial dealings, and provide ADR between the parties involved in such a complaint.¹¹ The Commission can also provide ADR to small businesses involved in disputes.¹² Under section 3 of the VSBC Act, “dispute” means a contractual or commercial dispute between a small business and another business, or another body referred to in that section.

For the purposes of the VSBC Act, ADR is defined to include mediation and preliminary assistance.¹³

The Commission also has the power to make representations to an appropriate person or body on behalf of a small business who has made a complaint.¹⁴

New South Wales Small Business Commissioner

The NSW Small Business Commission was established under the *Small Business Commissioner Act 2013* (NSW) (‘NSW SBC Act’).

The Commissioner can receive and deal with complaints made by or on behalf of small businesses regarding dealings with other businesses.¹⁵ Such complaints must:

- relate to the unfair treatment of, or an unfair practice involving, the small business; or
- relate to an unfair contract to which the small business is a party; or
- be in the public interest to deal with.¹⁶

The Commissioner’s functions also include the provision of low cost ADR services for small businesses, and making representations or taking any action on behalf of small businesses (including making applications to be joined as a party in proceedings involving a small business).¹⁷

The Commissioner can issue a notice requiring attendance at mediation for the purposes of resolving a complaint or other dispute involving small business. Failure or refusal to attend compulsory mediation attracts a maximum penalty of 100 penalty units for corporations or 50 penalty units for individuals.¹⁸

While the NSW SBC Act does not define ADR, and only makes explicit reference to mediation, the Commissioner’s objectives include facilitating resolution of disputes “through mediation and other appropriate forms of alternative dispute resolution”.¹⁹

Analysis

For small businesses in jurisdictions with a small business body, this is potentially the most efficient pathway for external escalation of an issue that falls within the body’s remit. However, the fact that the ASBFEO also deals with these issues is likely to make it unclear which pathway small businesses should take.

This could be improved by educating small businesses about which pathways are open to them for the different types of in-scope issues, and what each body is able to do in response to complaints. Additionally, a ‘no closed door’ approach where agencies internally refer complainants to the most appropriate agency would assist with this.

¹¹ *Small Business Commission Act 2017* (Vic) s 5(2)(c).

¹² *Small Business Commission Act 2017* (Vic) s 5(2)(e).

¹³ *Small Business Commission Act 2017* (Vic) s 3.

¹⁴ *Small Business Commission Act 2017* (Vic) s 5(2)(d).

¹⁵ *Small business Commissioner Act 2013* (NSW) s 14.

¹⁶ *Small business Commissioner Act 2013* (NSW) s 15.

¹⁷ *Small business Commissioner Act 2013* (NSW) s 14.

¹⁸ *Small business Commissioner Act 2013* (NSW) s 18.

¹⁹ *Small business Commissioner Act 2013* (NSW) s 13.

s47C - deliberative processes

Australian Consumer Law Regulators

The Australian Consumer Law ('ACL') – the primary mechanism through which Australian consumer rights are safeguarded – is contained within the *Competition and Consumer Act 2010* ('CCA'). It is enforced by federal, state and territory ACL regulators. At the federal level, the ACCC is the main regulator, while the Australian Securities and Investment Commission (ASIC) regulates financial products and services. Each state and territory has its own consumer protection body, with its own enabling legislation that sets out its functions and powers. The ACL is enforced by all Australian courts and tribunals.²⁰

What does the ACL cover?

Relevantly, provisions of the ACL include:

- protections against unfair contract terms in standard form consumer and small business contracts;
- protections against misleading or deceptive conduct and unconscionable conduct;
- protection against other unfair business practices; and
- consumer guarantees when purchasing goods and services.

The table below outlines which in-scope issues the ACL regulators may have authority to deal with.

Figure 1. Provisions of the ACL that are potentially breached by in-scope digital platform issues

In-Scope Issue	Description	ACL Provisions that may be relevant
Payment and transaction issues between users	<i>Payment and transaction issues between users, on a platform that has a payment system or functions as a marketplace.</i>	<ul style="list-style-type: none"> • Wrongly accepting payments – e.g. seller accepting payment when goods and services are materially different to what was paid for. • Excessive payment surcharges – i.e. excessive surcharges that do not reflect the cost of using the payment methods for which they are charged. • Prohibitions on Misleading or deceptive conduct and false or misleading representations in the provision of financial products and services under the <i>ASIC Act</i> and the <i>Corporations Act</i>.
Spam	<i>Content that is unsolicited, annoying and usually posted or sent in bulk to users.</i>	<ul style="list-style-type: none"> • Nil
Scams	<i>Content that is false and designed to trick users into spending money, sharing their personal information etc. Includes online shopping, investment, dating scams, fake ads and phishing.</i>	<ul style="list-style-type: none"> • Misleading or deceptive conduct. • False or misleading representations. • Participation in a pyramid scheme. • Assertion of right to payment for unsolicited goods or services.

²⁰ [Australian Consumer Law](#)

In-Scope Issue	Description	ACL Provisions that may be relevant
		<ul style="list-style-type: none"> • Harassment or coercion. • Bait advertising – i.e. offering promotions that they cannot honour. • Offering rebates, gifts, prizes etc. – i.e. offering any rebate, gift, prize or other free item with the intention of not providing it, or of not providing it as offered. • Drip pricing – e.g. claiming products are for sale at a very low price which does not include additional fees, charges and taxes that must also be paid. <p>“Many scams, if tested in court, may be breaches of the ACL. However, due to the ‘fly by night’ nature of many scammers, it is extremely difficult for law enforcement agencies to track them down and take action against them. This is further complicated by the fact that most scammers are based overseas.”²¹</p>
Fake reviews	<i>Fake reviews or comments e.g. fake reviews on a business page to boost sales, or fake, vexatious complaints received from unsatisfied customers.</i>	<ul style="list-style-type: none"> • Misleading or deceptive conduct • False or misleading representations
Hacking and fake accounts	<i>Account hacking or fake accounts created to mimic another user, or fake accounts created to engage in offensive or inauthentic behaviour.</i>	<ul style="list-style-type: none"> • Misleading or deceptive conduct • False or misleading representations • Harassment or coercion
Account and content removal	<i>When a platform suspends or removes an account, or removes content posted by a user. For businesses this can result in loss of followers or customer data on the platform.</i>	<ul style="list-style-type: none"> • Unfair contract terms – e.g. terms enabling one party to terminate the contract for trivial breaches, or penalise the other party for breaching the contract. Or e.g. a term that limits one party’s rights to sue another party and terms that require a consumer to bring legal proceedings or compulsory arbitration in a foreign jurisdiction may be unfair.
Ad-related issues	<i>Issues around ads such as being incorrectly billed for an ad, ad not delivering promised or expected results, transparency around ad effectiveness and unexpected changes to platform algorithms that reduce ad visibility.</i>	<ul style="list-style-type: none"> • Unfair contract terms or unconscionable conduct. <p>Additionally, if the issue relates to purchased ads not delivering promised results, or if representations have been made about the effectiveness of an ad, this may constitute:</p> <ul style="list-style-type: none"> • Misleading or deceptive conduct • False or misleading representations

²¹ ACCC [Scamwatch](#)

In-Scope Issue	Description	ACL Provisions that may be relevant
Issues around platforms' complaint handling policies and procedures	<i>Issues that users have with the platform's complaint handling policies and processes. Examples include where users couldn't find information on how to make a complaint or contact the platform and where users were told they were in breach of platform guidelines but didn't know which provision.</i>	<ul style="list-style-type: none"> Unfair contract terms – e.g. A term that allows one party unilaterally to determine whether the contract has been breached or to interpret its meaning. Or e.g. a term that limits one party's rights to sue another party and terms that require a consumer to bring legal proceedings in a foreign court may be unfair. Or e.g. terms enabling one party to terminate the contract for trivial breaches, or penalise the other party for breaching the contract. Or e.g. a term that limits one party's rights to sue another party and terms that require a consumer to bring legal proceedings or compulsory arbitration in a foreign jurisdiction may be unfair. Unconscionable conduct – e.g. conduct that is unconscionable based on factors including the relative bargaining strength of the parties, the use of undue influence, pressure or unfair tactics by the stronger party, and whether any conditions were imposed on the weaker party that were not reasonably necessary to protect the legitimate interests of the stronger party.

Enforcement powers and remedies

The enforcement powers, penalties and remedies that can apply to breaches or suspected breaches are contained in Chapter 5 of the ACL. For in-scope digital platform issues, the ACL regulators would only have powers to assist if they believe an issue constitutes a breach of the ACL (or the CCA more broadly for the ACCC). The ACL regulators cannot make a decision as to whether a person or business has in fact breached the law, this must be determined by a court.

Most enforcement mechanisms in Chapter 5 require a court or tribunal to determine that a breach has occurred. There are, however, a number of compliance options open to ACL regulators that do not require a court to determine that a breach has occurred. These include:

- Enforceable undertakings** – where there is a potential breach of the ACL, a person may offer the ACL regulator an undertaking that they will not repeat the breach and will take steps to comply. If the regulator accepts the undertaking, it is enforceable in court;
- Substantiation notices** – regulators can issue notices to businesses seeking information and documents about claims made in the marketplace to determine if they are genuine or whether further investigation is necessary; and
- Public warning notices** – if a regulator has reasonable grounds to suspect a breach of the ACL, including failing or refusing to respond to a substantiation notice, the regulator can issue a public warning notice.

Other remedies that require a court to be satisfied that a breach has occurred, or will occur, include:

- Civil pecuniary penalties;**
- Injunctions;**
- Damages;**

- **Compensation orders;**
- **Adverse publicity orders** – such orders require the contravening person to publish information at their own expense;
- **Disqualification orders** – ACL regulators can apply for an order disqualifying a person from managing a corporation due to breaches of the ACL;
- **Declarations** – the court can declare a term of a consumer or small business contract unfair on application by a party to the contract or an ACL regulator. If a term is declared ‘unfair’, it will be void;
- **Non-punitive orders** – the court can order a person who has engaged in contravening conduct to perform a service that relates to that conduct, for the benefit of the community;
- **Redress for non-parties** – ACL regulators can seek orders (other than for damages) to remedy or prevent loss or damage suffered by a class of persons, without first establishing the identity of those persons whom the breach affected; and
- **Other orders** to vary or void contracts.

The NSW Fair Trading Compliance and Enforcement Policy states that in deciding whether to pursue matters, ACL regulators take into account the cost benefit analysis of undertaking enforcement action and the likelihood of a successful outcome; the seriousness of the breach and/or consumer detriment; and the likelihood of achieving compliance using the level of enforcement undertaken.²²

ACL regulators are less likely to pursue enforcement where the issue is an isolated event.²³

The formal powers of the ACCC, and of the NSW Fair Trading and Consumer Affairs Victoria as examples of state and territory bodies, are set out below.

Australian Competition and Consumer Commission (ACCC)

The ACCC is an independent Commonwealth statutory authority. Its primary role is to enforce the CCA. It also regulates national infrastructure services.

The ACCC has powers under the CCA to:

- conduct research and studies into matters referred to it (including compulsory information gathering powers);
- Investigate and bring enforcement action against parties suspected of breaching the CCA;
- critically examine laws protecting the interests of consumers;
- make information available to the public on matters affecting the interests of consumers; and
- provide guidance on the rights and obligations that exist under laws designed to protect consumers.

While it has the power to do so, the ACCC does not currently resolve individual consumer complaints. As an authority enforcing legislation, the ACCC does not have the power to determine if a party has contravened the CCA (a power reserved to the Courts under Australia’s Constitution). As a result, the ACCC is not designed to be able to address the over 300,000 contacts it receives annually. It does not act on behalf of or provide legal advice to consumer on their rights and obligations under the law in relation to individual complaints.²⁴ Rather it uses information provided to it to help understand what issues are causing most harm to Australian business and consumers. This helps it to focus compliance and enforcement efforts.²⁵

Breaches of the CCA can include misuse of market power; entering contracts or arrangements that restrict competition; contravention of industry codes; and breaches of the ACL. Where the ACCC believes there has been a contravention of the CCA, it can pursue formal sanctions such as infringement notices, enforceable undertakings, and court action

²² [NWS Fair Trading Compliance and Enforcement Policy, July 2013 \(nsw.gov.au\)](#)

²³ [ACCC Compliance and Enforcement Policy](#)

²⁴ [What we can & can't do for consumers | ACCC](#)

²⁵ [Where to go for consumer help | ACCC](#)

(including criminal penalties for cartel conduct). The enforcement powers and remedies available to ACL regulators in response to breaches of the ACL are set out above.

Scamwatch

Scamwatch is an ACCC-run website that provides a wealth of information to consumers and small businesses about how to recognise, avoid and report scams. It contains scams information in 12 languages other than English. Scamwatch uses scam reports to spot emerging issues, and it warns the public through media releases, social media updates and radar alerts. It also engages with the community at public forums and events to provide more targeted messaging for particular groups—such as prioritising emerging issues affecting vulnerable and disadvantaged consumers. However, it has no powers to respond to individual complaints or offer assistance or legal advice about specific issues.

The ACCC monitors scam reports and, where appropriate, shares intelligence from reports with other government agencies, law enforcement and private organisations. Scamwatch engages with businesses that scammers use to source victims or receive money through—for example, social media platforms, online shopping platforms, financial intermediaries and telecommunications businesses. The ACCC encourages these private organisations to monitor scams, raise awareness and disrupt scams that occur on or via their services.

State and Territory Consumer Protection Bodies

Consumers can make complaints to their state or territory's ACL regulator. The first step in the resolution process through these bodies is usually to encourage the consumer to resolve the dispute informally with the business.

New South Wales Fair Trading

Fair Trading is a Division of the NSW Department of Customer Service that aims to create a fair, safe and equitable marketplace in NSW. It may investigate alleged breaches of all legislation it administers. Fair Trading is the state's regulator of the ACL under the *Fair Trading Act 1987* (NSW).

Of the matters handled by Fair Trading, those that may relate to digital platforms include breaches of the ACL, and breaches by booking platforms of the Code of Conduct for Short-Term Rental Accommodation industry.²⁶

For breaches of the ACL, Fair Trading has a variety of enforcement options open to it, ranging from warnings and enforceable undertakings to civil pecuniary penalties and criminal proceedings.

Consumer Affairs Victoria

Consumer Affairs Victoria (CAV) is part of the Victorian Department of Justice and Community Safety. It is led by the Director of Consumer Affairs, which is a statutory office created under the *Australian Consumer Law and Fair Trading Act 2021* (Vic) ('ACLFTA').

CAV does not have binding decision-making powers, and cannot force people to participate in dispute services. Its key objective being voluntary compliance.²⁷ The ACLFTA gives the Director power to receive complaints about, and refer to mediation or conciliation, disputes between purchasers or consumers and suppliers.²⁸ CAV employees conduct the mediation or conciliation. The Director can also institute court proceedings on behalf of any persons in respect of a consumer dispute.²⁹

²⁶ [Booking platform obligations | NSW Fair Trading](#)

²⁷ [Consumer Affairs Victoria Regulatory Approach and Compliance Policy](#)

²⁸ *Australian Consumer Law and Fair Trading Act 2021* (Vic) s 114.

²⁹ *Australian Consumer Law and Fair Trading Act 2021* (Vic) s 115.

In practice, CAV's primary dispute service is delivered by telephone. In limited circumstances, it offers conciliation services.³⁰

CAV also uses a range of other compliance and enforcement options:

- **Education letter** – where a previously cooperative business appears not to be aware of a potential breach.
- **Without prejudice discussion** – seeking prompt resolution of alleged non-compliance without resorting to court or tribunal involvement.
- **Business compliance program** – a voluntary program targeted towards businesses with a high or disproportionate number of contacts to ACL regulators. CAV is more likely to target businesses with inadequate complaints handling or which raise other systemic issues. Businesses agree to an action plan.
- **Compliance monitoring** – to detect breaches of the law.
- **Warning letter** – when a business can be reasonably expected to know and understand their obligations.
- **Infringement notice** – asserts a breach of the law and imposes a financial penalty. This allows straightforward breaches to be dealt with by paying a fine, rather than court proceedings.
- **Public statements** – CAV uses public statements particularly as a timely and effect tool to prevent ongoing consumer harm from widespread issues, and where lengthy court proceedings are ongoing. Statements include:
 - Consumer warning notices including about unfair business practices and other consumer risks;
 - Industry warning notices about CAV's intentions for compliance activities; and
 - Reporting contacts, disputes, infringements and other data and information that the CAV holds.
- **Enforceable undertakings** – as an administrative alternative to court action.
- **Civil proceedings and criminal prosecution.**

Analysis

ACL regulators have a number of compliance and enforcement powers open to them, which could be employed in response to all complaints from consumers about potential breaches of the law. However, in practice these are reserved for significant and systemic breaches.

The ACCC cannot pursue all the complaints it receives about the conduct of traders or businesses and the ACCC rarely becomes involved in resolving individual consumer or small business disputes. While all complaints are carefully considered, the ACCC's role is to focus on those circumstances that will, or have the potential to, harm the competitive process or result in widespread consumer detriment. The ACCC therefore exercises its discretion to direct resources to the investigation and resolution of matters that provide the greatest overall benefit for competition and consumers.³¹

The regulators' decision not to pursue action in individual cases is largely due to the resource intensive nature of bringing action before a court or tribunal, as is required to determine whether breaches have occurred.

Court action can be a very long process, particularly given platforms may appeal decisions. It is therefore not a satisfactory resolution option for individuals or small businesses experiencing a one-off issue. Pursuing a resolution through an ACL regulator is not appropriate for time-sensitive issues, or to avoid immediate loss and damage caused by issues such as being locked out of an account or receiving fake reviews.

As outlined above, the ACL regulators also have a number of enforcement options open to them for potential breaches that do not require court determinations. These include enforceable undertakings, substantiation notices, and public warning notices. These are also used sparingly – for example, 21 section 87B undertakings were accepted and one public warning notice was issued in 2020.³² None of these were received by or issued against major digital platforms. This may

³⁰ [Consumer Affairs Victoria Regulatory Approach and Compliance Policy](#), p 8.

³¹ [ACCC Compliance and Enforcement Policy](#), p 2.

³² [ACCC Public Registers](#)

be partly because the option to bring an issue before a court is seen as a more effective deterrent. These administrative enforcement options focus on deterrence, rather than resolving an individual issue in a manner that is likely to be satisfactory to the complainant.

While pursuing a resolution through an ACL regulator may be an option, the powers of the regulators would be better employed to address the underlying practices that cause individuals to experience in-scope issues.

ACL regulators should address the underlying practices that cause in-scope issues

While some issues may be better pursued as private actions, such as payment issues between two users, many of the in-scope issues stem from conduct which is prohibited under the ACL.

As such, while pursuing a resolution through an ACL regulator may not lead to a satisfying or timely resolution for an individual, increased use of enforcement powers and remedies by the regulators in response to individual complaints could positively address competition and consumer protection issues in general.

For example, content or account removal issues may become disputes because of contract terms that allow the platform to unilaterally determine whether the contract has been breached, such as when little specificity is provided about alleged breaches of terms and conditions. The ACL regulators could pursue enforcement action (i.e. seek declaration that the terms are void) more often in response to individual complaints of this issue, indicating more willingness to enforce consumer protections and encouraging a shift in the conduct of digital platforms. Terms that are declared void can be voided for all iterations of that standard form contract. This means that a term could be void, for example, for all users of a platform who have accepted the same terms and conditions.

Similarly, terms that allow one party (but not the other) to terminate the contract, for example in response to an inconsequential breach by the consumer, may be the cause of account removal disputes. Terms that limit one party's ability to sue, or require a consumer to bring legal proceedings or compulsorily engage in arbitration in a foreign jurisdiction may also be unfair. Law reforms to impose substantial penalties for contraventions of the unfair contract term prohibition (as is the case for other ACL provisions) would incentivise platforms to engage in fair and competitive conduct.

s47C - deliberative processes

Office of the eSafety Commissioner

The Office of the eSafety Commissioner was established as an independent statutory office under the *Enhancing Online Safety Act 2015* (Cth). It currently only has power to deal with out-of-scope issues; however, receives complaints about many in-scope issues. These include hacking and fake accounts, fake reviews, scams, issues around platform complaint handling policies, and account and content removal and procedures. In responding to these complaints, the Office of the eSafety Commissioner relies upon informal powers and informal relationships with platforms.

The *Online Safety Act 2021* (Cth) may provide mechanisms that the Office of eSafety Commissioner can use in the future. The Act introduces a means by which 'Basic Online Safety Expectations' (BOSE) for social media services, relevant electronic services and designated internet services, can be established by legislative instrument.³³ The BOSE would be administered and regulated by the eSafety Commissioner.

³³ *Online Safety Act 2021* (Cth) Part 4.

The core BOSE relate only to measures to address harmful online content and user safety, and therefore do not directly address the breadth of in-scope issues. However, the *Online Safety Act* includes powers for the Minister for Communications to determine additional Expectations, which could cover in-scope issues.

Where a service provider does not meet these Expectations, the eSafety Commissioner may publish a statement to that effect on the Commissioner's website.³⁴

Office of the Australian Information Commissioner (OAIC)

The OAIC is an independent agency within the Attorney-General's portfolio. It was established under the *Australian Information Commissioner Act 2010* (Cth). The OAIC is responsible for the privacy functions conferred by the *Privacy Act 1988* (Cth) and other laws; and administering the *Freedom of Information Act 1982* (Cth).

Some in-scope issues deal with privacy-related issues, such as hacking and fake accounts. However, the OAIC's functions relate specifically to an organisation's handling of personal information, whereas hacking and fake account issues are user-to-user issues. Issues stemming from a platform's handling of personal information are out-of-scope of this project.

³⁴ *Online Safety Act 2021* (Cth) s 48.