

**To regulate or not to regulate: unravelling institutional tussles around the regulation of
algorithmic control of digital platforms**

Olga Kokshagina*

Faculty for Strategy, Entrepreneurship and Operations

EDHEC Business School, France

olga.kokshagina@edhec.edu

Pauline C. Reinecke*

Institute for Strategic and International Management

Hamburg University of Technology, Germany

pauline.reinecke@tuhh.de

Stan Karanasios

School of Business

University of Queensland, Australia

s.karanasios@uq.edu.au

* The first two authors contributed equally and are listed alphabetically.

Version of July 4, 2022

Accepted for publication at *Journal of Information Technology*

We thank our Editor and anonymous Reviewers for their developmental feedback. Previous versions of this manuscript also benefited from fruitful comments from Charlotte Cloutier, Michael Smets and Thomas Wrona as well as from attendees of the International Conference of Information Systems (ICIS) 2020, the European Conference of Information Systems (ECIS) 2021 and the European Group of Organization Studies (EGOS) Colloquium 2021.

This work was supported by the Horizon 2020 Programme of the European Union within the OpenInnoTrain project under grant agreement n 823971. The content of this publication does not reflect the official opinion of the European Union. Responsibility for the information and views expressed in the publication lies entirely with the authors.

To regulate or not to regulate: unravelling institutional tussles around the regulation of algorithmic control of digital platforms

Abstract

Regulating how digital platforms use algorithms to determine and control content displayed to their users is both a controversial topic and an important societal challenge. Existing research acknowledges institutional tussles around regulating how digital platforms use algorithms to determine and control content. However, we lack research showing how the development of regulation unfolds. We build on data from a longitudinal discourse analysis of 410 media articles and 483 policy and industry documents to study two cases of algorithmic control regulation in Australia. The first involves algorithmic control for content display, the second for content moderation. We develop a process model of institutional work towards regulation of algorithmic control. It captures the institutional tussles between governments, digital platforms and third parties as each expresses their perspective on legitimate forms of algorithmic control and shapes the process and outcome of regulation. Building on our model, we discuss the dynamics of regulation development in light of the constellation of actors and their power position in the process. We further consider the regulatory outcome and highlight future research questions that build on our findings.

Keywords: *algorithmic control, digital platforms, institutional work, regulation process*

1 Introduction

Digital platform firms such as Google or Facebook (hereafter: digital platforms) provide increasingly ubiquitous services across many areas of modern society (Bailey et al., 2022). Algorithms are at the core of digital platform business models, determining and controlling the content displayed to users. As algorithms become more present in everyday life, the expectation they will conform to social values increases (Bellanova and de Goede, 2022).

Various events have drawn public attention to problems of algorithmic control, including the algorithmic recommendation of fake news (Khan et al., 2021) or terrorist content (Rauf, 2021) or the manipulation of elections through algorithmic profiling (Kim and Routledge, 2022). In 2021, the whistleblower Frances Haugen sparked debate about algorithmic control, claiming that “[Facebook’s] systems for detecting objectionable content such as hate speech detect only a very small minority of objectionable content. Because the company is heavily focused on scaling, it is unlikely to ever catch more than 10% to 20% of infringing content” (UPI, 2021).

These issues have been the focus of various regulatory debates (Parra et al., 2021) such as regulation of automated algorithmic decision-making (Marjanovic et al., 2021), algorithmic audiencing on social media platforms (Riemer and Peter, 2021), algorithmic control on online labor platforms (Möhlmann et al., 2021) or accountability of AI-based applications (Asatiani et al., 2020). Governments have responded by developing regulations including the *Digital Market Acts* (DMA) and the *Digital Services Acts* (DSA) in Europe, and amendments to the *Criminal Code* and the *Competition and Consumer Act* in Australia. Digital platforms have responded by using their extraordinary economic, social, and political power to shape regulation, turning to self-regulation as a means to preempt governmental regulation and restore their practical legitimacy (Boon et al., 2019; Cusumano et al. 2021).

Both regulation and self-regulation are subject to high institutional complexity. They are influenced by rapid technological developments and the different interests and power positions of stakeholders, including digital platforms, governments and (non-) commercial end-users (Boon et al., 2019; Riemer and Peter, 2021). The diversity of stakeholder positions and roles has resulted in frequent tussles over regulation of algorithmic control (Pandey et al., 2022; Zuboff, 2015) and criticism of both approaches (Common, 2020). As such, finding effective ways to regulate the use of algorithms by digital platforms is an important research gap (Mikalef et al., 2021; Parra et al., 2021). However, it remains unclear how regulation is negotiated and how stakeholders shape regulation outcomes. Informed by the theory of institutional work and motivated by the urgent need for regulation of algorithmic control of digital platforms, we ask: *How does the institutional work of stakeholders unfold in the development of regulation of the use of algorithmic control of content by digital platforms?*

To study these unfolding dynamics, we draw on data from media, policy and industry documents. We analyze the institutional work of stakeholders in two revelatory cases (Leonard-Barton, 1990; Yin, 2014) involving regulation of algorithmic control of (i) news media content; and (ii) extremist and terrorist content. We show that developing regulation is collective institutional work by different actors. Further, both the process and regulatory outcome are influenced by institutional tussles over the legitimate form of algorithmic control.

We contribute to the emerging IS literature on regulation of algorithmic control by digital platforms and advance theory about institutional work for disruptive technology regulation in three ways. First, our model captures the pluralistic institutional work required to regulate digital platforms' use of algorithms and shows how the regulation process unfolds over time. Second, we reveal the tension between the institutional work of government and the practical

legitimacy of digital platforms, and how the latter can be a barrier to regulation. Third, we nuance the interplay of regulation and self-regulation of algorithmic control by highlighting how actors' intentions and implementation of each diverge, thereby impacting regulation. Our study also informs policymaking processes for regulation of algorithmic control.

2 Literature review

2.1 Algorithmic control of content display and moderation

Digital platforms can be seen as socio-technical systems composed of users, algorithms, and content. Digital platforms have become important spaces for social interaction as they bring individuals and organizations together, orchestrate the relations between them, and enable user communication and content display (Zuboff, 2015). They then depend on algorithms to analyze data about users and to increase and commercialize user engagement through personalized content and advertising (Riemer and Peter 2021). Recently, digital platforms' use of algorithmic control gained attention in two key areas: (i) news curation (Khan et al., 2021; Riemer and Peter, 2021); and (ii) content moderation (Borelli, 2021; Rauf, 2021).

News curation is organized by algorithms that display customized news content to users in ways unknown to the user and the news provider (Rader and Gray, 2015). Such algorithmic control has been criticized recently for distorting news dissemination. This occurs by selecting audiences for particular news stories in automatic and opaque ways, or by suppressing content in unpredictable and undisclosed ways (Borelli, 2021; Riemer and Peter, 2021). Moreover, algorithms are able to create feedback loops that reinforce interests and biases and manipulate users, as with Cambridge Analytica (Cecez-Kecmanovic, 2019; Clarke, 2019).

Content moderation is required when content violates social rules, values, or norms (Riemer and Peter, 2021). Digital platforms have developed socio-technical governance systems for content moderation whereby users or algorithms report problematic content which is then further processed by a human content moderator or artificial intelligence to automate content detection and prevent further dissemination (Borelli, 2021; Gorwa et al., 2020). When the content is misjudged, newsworthy content may be removed or morally questionable content broadcast, meaning that content moderation straddles the line between free speech and censorship, as in the Napalm girl case (Common, 2020).

Such issues have prompted calls for regulation to bring more transparency and accountability around algorithmic control (Biggar and Heimler, 2021).

2.2 Regulating forms of algorithmic control of content

Attempts to regulate algorithmic control take place at the intersection of self-regulation by digital platforms and government regulation (Aragon-Correa et al., 2020; Berkowitz and Souchaud, 2019; Cusumano et al., 2021). Digital platforms such as Google and Facebook have opted for self-regulation when facing public pressure from policymakers, negative media coverage, and boycott of their systems by advertisers (Bellanova and de Goede, 2022; Borelli, 2021; Riemer and Peter, 2021). In doing so, they preempt government regulation that would force them to disclose their algorithms (Cusumano et al., 2021; Kwoka and Valletti, 2021), which are guarded as trade secrets (Common, 2020; Kim and Routledge, 2022). However, digital platforms experience a tension between economic goals and societal interests. Some digital platforms, for instance, promote sensationalist content to create higher user rates (Whittaker et al., 2021) and consequently higher profits (Cusumano et al., 2021).

Credible threats of government regulation can both induce and increase the effectiveness of self-regulation (Kwoka and Valletti, 2021). Governments may either adjust existing regulatory schemes (e.g. existing competition and data protection regulation, Jenny, 2021; Kira et al., 2021) or develop new regulations (Petit and Teece, 2021) to allocate responsibility and liability to digital platforms (Gurkaynak et al., 2016; Reed, 2018). However, governments face challenges to intervene effectively in the operation of digital platforms (Cusumano et al., 2021), both because algorithms are opaque and subject to constant changes, making outside regulation or supervision difficult (Bristows, 2018), and because poorly designed interventions may create harmful side effects for users, ecosystems, and the global digital economy (Petit and Teece, 2021).

In the recent years there have been multiple regulatory efforts by government to address content control issues. Examples include the *News Media and Digital Platforms Mandatory Bargaining Code* (Australia) and the *10th Amendment of the German Competition Act also known as GWB Digitalisation Act* (Germany) that both came into force in January 2021, and the recently passed DMA and DSA in Europe. Other governmental efforts for regulation of terrorist content moderation include the *German Network Enforcement Act (NetzDG)* passed in 2017, an amendment to the *Criminal Code on “Sharing of Abhorrent Violent Material”*, passed in Australia in 2019, and the *EU Regulation on “Addressing the dissemination of terrorist content online”* (EU 2021/784) passed in 2021 and supplemented by the DSA.

These developments highlight the complexity of regulating algorithmic control and indicate that institutions involved might disagree over what is the ‘right’ level of regulation.

2.3 Pluralistic institutional work in technology regulation

The process of regulating technology involves multiple stakeholders with diverse beliefs, capabilities, interests and goals (Pandey et al., 2022). Multiple institutions enable or constrain actors' behaviors in specific social systems (Friedland, 1991). Institutional theory emphasizes that these institutions are available for interpretation and active use by embedded actors who engage in purposeful interactions (Pache and Santos, 2010). On this basis, the process of technology regulation appears as a negotiation or tussle between multiple institutional demands (Goodrick and Reay, 2011) to arrive at the 'right' regulatory outcome (e.g., Boon et al., 2019; Fuenfschilling and Truffer, 2016). Actors will engage in that process and use their rhetorical capacities (Lawrence et al., 2013; Stewart et al., 2006) and power positions (Pache and Santos, 2010) to legitimize and impose their view of appropriate governance measures (Kraatz and Block, 2008).

Scholars have drawn on institutional work to study regulation (Pemer and Skjølsvik, 2018; Slager et al., 2012). Institutional work refers to categories of purposive action aimed at creating, maintaining and disrupting institutions (Stewart et al., 2006, see Table 1). Creating new institutions comprises practices devoted to creating new rules, norms and belief-systems. These may include defining and developing new regulations to allocate responsibility and liability to digital platforms or constructing normative networks and advocating for the importance of regulation. Maintaining institutions comprises practices to reproduce existing regulations, norms and belief-systems such as protection of institutions threatened by the use of algorithms by digital platforms. Disrupting institutions is carried out by actors who seek to change existing institutions. Disruption can be directed at existing regulations, norms or belief-systems through practices that undermine assumptions and beliefs. Digital platforms may disrupt institutions that harm their legality if they have the power to do so and it does not harm their legitimacy (Boon et al., 2019).

Insert Table 1

In practice, institutional work on regulation and technology is pluralistic, intertwined or even conflicting (Slager et al., 2012). Fuenfschilling and Truffer (2016) highlight how the co-evolution of technologies and institutions requires actors to (de)institutionalize certain regime structures so as to enable and influence a socio-technical transition. Pemer and Skjølsvik (2018) show that the implementation of a new regulation consists of regulators defining new practices and regulatees changing and adapting these practices to their local needs. Using the example of Airbnb, Boon et al. (2019) highlight regulation as the result of regulators confronting

proponents (i.e., digital platforms and their hosts legitimizing platform practices), and opponents (i.e., incumbents and non-users demonizing practices to maintain institutions).

These initial studies advance our understanding of what effect the presence of multiple actors has on institutional work around technology regulation. However, research on regulation currently lacks insight into the effect of pluralistic institutional work, negotiations, and tussles between multiple actors on both its development and outcomes.

3. Method

3.1 A longitudinal perspective: focus on two case studies

We chose a longitudinal, comparative case-study design to study the unfolding dynamics of inter-organizational institutional work towards regulation of algorithm use by digital platforms (Pettigrew, 1990). Using purposeful sampling (Patton, 2002), we selected two revelatory cases (Yin, 2014): Our first case is regulation of algorithmic control for news media content leading to *Australia's Treasury Laws Amendment (News Media and Digital Platforms Mandatory Bargaining Code) Act 2021* (hereafter “the code”). Our second case is regulation of algorithmic control of extremist and terrorist content on social media platforms resulting in an amendment to *Australia's Criminal Code* in 2019. These two cases were ideal for our theorizing as they allowed us to distinguish between idiosyncratic and general patterns, (Leonard-Barton, 1990), contributing to the robustness of our findings (Eisenhardt and Graebner, 2007). Both cases illustrate a process of negotiations for regulating algorithmic control taking place between multiple institutional actors and show how their interests played out in the public sphere. Both cases also resulted in a regulatory outcome, shifting responsibility for regulation from digital platforms to government. The cases do differ (Eisenhardt, 1989) in how the digital platforms were using algorithms (content display in case 1, content moderation in case 2), which government bodies were involved (the Australian Competition and Consumer Commission (ACCC) and the Australian Attorney-General's Department (AGD)), and the geographical reach of the discourse (national in case 1, international in case 2).

3.2 Research setting

Both cases are anchored in Australia. Studies of portrayals and regulation of algorithms and digital platforms normally focus on larger economies such as the U.S. and Europe (e.g., Boon et al., 2019; Chuan et al., 2019; Sun et al., 2020). Our focus on Australia was important for two reasons. First, Australia's national strategy for regulation of algorithms was at a formative stage, which allowed us to go beyond postliminary regulation to understand the interplay between digital platforms and other actors in shaping algorithmic control regulation. Second, focusing

on Australia, a smaller actor in the global digital platform landscape, enabled us to observe the influence of other countries, geopolitics, and digital platforms. As such, the setting is indicative of the challenges that other countries face in developing regulation.

Context - Case 1:

Australian news media rely on advertising to fund news and journalism. With the rise of digital platforms like Google and Facebook, the delivery and consumption of news has changed significantly. News media companies are now able to reach audiences and monetize their online content through advertising (ACCC, 2018). The total online advertising market in Australia has grown by A\$3.1 billion between 2014 and 2017, with Google and Facebook accounting for 70% of that growth. At the beginning of our research in 2018, over half of online news consumption in Australia was channeled through algorithm-driven platforms (Fisher et al., 2018). At that time, 26% fell to Google, 25% to Facebook and 4% to digital platforms such as Twitter, Apple News and Instagram (ACCC, 2018). Algorithms control how information is displayed based on user profiling and ongoing data collection. While consumers traditionally chose news based on quality and brand trust, their choice is now affected by the algorithmic preselection of content. In 2018, 69% of digital platform media users chose news content based on an 'interesting headline' (ACCC, 2018). This encouraged media companies to produce more sensational news to optimize content for digital platform algorithms at the expense of the quality and breadth of journalism (ACCC, 2019). Furthermore, opaque algorithmic positioning limits media companies' scope of action, resulting in a substantial shift in market power and decline in their advertising revenues. Media companies have therefore pushed the government to establish rules for fair market competition.

Context - Case 2:

In recent years, social media has overtaken internet forums as the preferred space for propaganda and radicalization (Weimann, 2000, 2014). Digital platforms such as Twitter, YouTube and Facebook are increasingly used by terror groups to post content, including real-time streaming of terrorist attacks, and to seek potential recruits (Klausen, 2015). In 2015, the Australian Government formulated a counterterrorism strategy to protect society from terrorist attacks. The government significantly boosted resource deployments for security agencies and supplemented their hard counterterrorism (CT) strategies (i.e. disrupting terrorism through intelligence, military action, and law enforcement) with softer measures countering violent extremism (CVE) that aimed at counter- radicalization, especially on social media (Australia's CT Strategy, 2015). CVE involved a wide range of civil society actors and international

governments such as the Five Eyes alliance (consisting of the US, Australia, UK, Canada and New Zealand), G7 and G20 nations (Borelli, 2021; Ganesh and Bright, 2020). While digital platforms were initially reluctant to engage with the politics inherent to terrorism, this has shifted. Platforms have gradually moved from an ideological position promoting free expression and an uncensored internet (Rauf, 2021) to prohibiting extremist and terrorist content on their digital platforms by giving users reporting capabilities. This has been complemented with more active monitoring through algorithms and specific rules (“Twitter Rules”, “Community Standards” for Facebook, and “Community Guidelines” for YouTube).

3.3 Data collection

Recognizing that institutional work is language-centered (Stewart et al., 2006), we undertook qualitative discourse analysis. Our data was collected from multiple data sources (media articles, policy and industry documents) that constitute a discourse and capture the multiple stakeholders and their articulated views on algorithmic control (Fairclough, 1995; Van Dijk, 1990). Similar to other cross-document analyses of technology debates and discourses (Cukier et al., 2009; Rinta-Kahila et al., 2021; Rowe et al., 2020), triangulation of different data sources allowed us to counter the limitation of relying on one media source. Moreover, secondary data served as substitutes for records of activity that we could not observe directly. They helped us to avoid possible biases that may occur in real-time case studies, where different stakeholders distort events or engage in impression management (Ghazawneh and Henfridsson, 2012).

Media articles. Media texts are a common data source in discourse analysis (Fairclough, 1995; Joutsenvirta and Vaara, 2015; Van Dijk, 1990). They reflect the “institutional debate on values and political action and for scientific positions that inform the government and the public” (Rowe et al., 2020, p. 548).

The discourse on regulation of digital platforms and algorithmic control is embedded in broader societal discourse about the role of digital platforms, the development of algorithms and AI, and the need for regulation by governments. This general context is important to understand as it shapes the emotions and subjective positions of the discourse; for this reason, we used media articles as our first source to capture both discourses.

In line with studies that used the most widely read daily newspapers (e.g., The Australian (Rinta-Kahila et al., 2021), Le Monde (Rowe et al., 2020), The New York Times (Fast and Horvitz, 2017)), we started data collection using the national newspaper *The Australian*.

We used the ProQuest database to retrieve and download articles during our designated period of analysis (2015 – 2022). Out of 805 articles, we identified relevant articles that either closely

related to the discourse on regulation of digital platforms and algorithmic control, or captured broader societal discourse on the role of digital platforms in society, the development of algorithms, and the need for regulation. These articles can be seen as shaping the emotional and subjective positioning of the discourse. The research team engaged with the articles and compared our understanding of issues related to regulation of digital platforms, ultimately collecting 410 articles referring to the regulation context, of which 269 articles were chosen for detailed coding of two cases.

Policy and industry documents. We collected government policy documents and industry publications (Ghazawneh and Henfridsson, 2012) to gain insights into views and assumptions of the main participants in discourse on regulation, some of which were identified from the media articles. For case 1, for example, we collected all the documents that were part of the ACCC digital platform public inquiry, including submissions to the inquiry, concept notes and preliminary and final reports. This phase of data collection resulted in 483 documents for analysis (see Table 2).

Insert Table 2

3.4. Data analysis

We followed a two-step approach to analyze our data. This began with a procedural analysis and coding of the two cases, followed by a comparative analysis of two cases.

In the first stage, we conducted a detailed analysis of our data to construct a timeline of relevant events and develop rich description of two cases (Rinta-Kahila et al., 2021). We then coded our data using a discourse analysis coding scheme from the field of social policy debates (Creed et al., 2002a; Creed et al., 2002b). This captured: the problem definition (e.g., concerns about algorithm use by digital platforms); main stakeholders; problem elaboration, diagnoses, and motivations (institutional work); solution orientations and actions (e.g., normative, regulatory measures); and key events (e.g., governmental inquiry, Christchurch event). We arranged the data chronologically by year. Building on the literature on public policy processes (Rinfret et al., 2021), we identified four phases to structure our findings: discourse initiation (i.e., problem definition); discourse anchoring (i.e., agenda setting, debating governance measures with stakeholders); discourse legitimation (i.e., assessing different solutions); and regulatory outcomes (see Tables 3 and 4). To ensure the rigor of our coding, we adopted an insider-outsider approach. At the time of analysis one author was Australian/based in Australia, one was an international working in Australia, and another was based in Europe. This combination of perspectives ensured contextual knowledge while enabling us to ask critical questions.

The second stage of analysis used the results derived from our coding to compare and contrast the temporal dynamics of the two processes of institutional work. This allowed us to ascertain the mechanism underlying the identified dynamics. We went back and forth between data and literature on institutional work (Stewart et al., 2006) and technology regulation (Boon et al., 2019; Perner and Skjølsvik, 2018) in an iterative process to build on existing literature, identify recurring concepts, and develop novel insights on how the discourses on regulation of algorithmic control grow and mature over time.

Insert Table 3 and Table 4

4 Findings

Our findings capture two intertwined discourses on regulation of content, specifically how digital platforms use algorithms: (i) to determine news media content to display and (ii) to filter and control extremist and terrorist content. In the following sections we reveal findings on the purposeful institutional work of multiple actors, focusing on how this work evolves over time through pluralistic institutional collision, and the resulting effect on regulation.

4.1 Case 1: Algorithmic control of news media content

In 2017 the Australian federal treasurer commissioned the ACCC to conduct an inquiry into how digital platforms use algorithmic control to display news media content in order to understand the impact on competition in the media and advertising services markets. The government was pushed to act by traditional media companies who were seeking compensation from platforms. The ACCC's work on regulation formed part of a package of reforms to modernize and update Australia's media laws on the basis that "*the influence, significance and size of Google and Facebook has resulted in them being the principal focus on the inquiry*" (ACCC, 2018).

4.1.1 Algorithmic control of news media content – discourse initiation (2017 – 2018)

In 2017 the Australian Government expressed concerns over:

Google and Facebook which control 84% of all digital advertising and what impact they are having on others....; Google happened and is destroying journalism and Facebook happened and became a way for foreign governments to pervert elections (Former prime minister Scott Morrison 20/04/2018).

The inquiry allowed the ACCC to use compulsory information-gathering powers, hold hearings to assess the level of competition in the market, and examine the information asymmetries

between government/citizens, media companies and digital platforms around algorithmic control of content:

Algorithms determine the positioning of advertising on Facebook pages and the ranking of news reports in Google search-results. Yet nobody, apart from those at the tech giants, has any idea about the settings that determine the sort of news they present and the effectiveness of their advertising (The Australian 15/12/2018).

The ACCC aimed to define and create rules that will facilitate, supplement, and support fair and transparent competition in the media and advertising services markets. Here the institutional work of government is focused on thwarting threats to existing institutions, in particular ensuring fair market competition and quality journalism.

The ACCC's institutional work started by *defining* and *enabling* work, spurred on by media companies calling for “*a restraint on digital platforms' use of publishers' content unless they provide fair compensation*” (The Australian 11/12/2018) and academia promoting the need for disclosure of granular, useful information about the operation of a digital platform.

4.1.2 Algorithmic control of news media content— discourse anchoring (2018 – 2019)

The ACCC's *advocacy* work embodied concerns around market power imbalances and quality journalism by engaging with digital platforms, media companies and civil society to inform new rule systems that would maintain and/or adjust the *Competition and Consumer Act 2010*. The inquiry helped the ACCC to construct a *normative network* of experts from academia, media companies, industry, and public associations (e.g., Australian Association of National Advertisers). These experts supported the government's institutional work through their submissions to the inquiry and reinforced the need for clear standards to ensure disclosure of granular and useful information about digital platform operations: “*Google and Facebook were not subjected to the same rigorous and independent auditing as traditional media companies*” (News Corp submission 20/04/2018).

Media companies in particular expressed concerns about digital platforms increasing mediation of the relationship between publishers and consumers. They argued that this makes it difficult for traditional news organizations to offer original and quality news to consumers. At this stage media companies did not necessarily argue for regulation, but suggested normative interventions to address the negative impacts of algorithmic control such as establishing an “Algorithmic Review Board” to analyze and remedy algorithmic distortions of competition (News Corp submission 20/04/2018).

Based on 70 submissions, ACCC formulated potential rules and recommendations for regulating the use of algorithms by digital platforms. The report that was published on February 26, 2018 and emphasized that “*algorithms used by platforms to decide the prominence of news stories are opaque and regulatory investigation is needed to provide assurance to media companies*” (The Australian 11/12/2018). The report recommended addressing the market power of digital platforms through strengthened merger laws and processes and through amendments to privacy legislation to address use and collection of personal information.

The digital platforms initially welcomed the ACCC inquiry. Managing Director of Google Australia and New Zealand at the time, Jason Pellegrino, legitimized and aligned himself with the inquiry:

I’m actually really encouraged by the process ... Our industry, us as a business, the ecosystem, more broadly, technology has changed so rapidly over the last 10 years ... the review will just put some facts on the same table that are correct, because there’s a lot of misinterpretation (The Australian 06/01/2018).

Despite this initial support, digital platforms then undermined the institutional work of the ACCC by legitimizing their own practices. They built on *mimicry and education* to shield algorithmic control from criticism, arguing that algorithmic control provided the best possible service for users and media companies and promoted free and dynamic competition. For example, Google emphasized that their business model assists media companies to distribute and monetize their content, thereby supporting the growth of publishers (Google submission 20/04/2018). Facebook insisted on the benefits that online media create for people, journalists, media companies, and advertisers: “*Facebook helps people discover content that is meaningful to them*” (Facebook’s submission 18/04/2008).

4.1.3 Algorithmic control of news media content – discourse legitimation (2019 – 2020)

Following the publication of its preliminary report, the ACCC continued *advocating for and constructing normative networks* to determine which outcome was to be put in place. Further submissions were invited up to February 15, 2019, with events organized by the ACCC to collect feedback and additional submissions. The ACCC attempted to legitimize their recommendations with different stakeholders and establish a strong network around regulation, leading to a final inquiry report in July 2019.

Media companies such as News Corp expressed strong views on the impact algorithmic control has on their ability to monetize content. They noted that these algorithms are opaque, calling for digital platforms to provide transparency over major changes. For example, a News Corp

executive chairman stated: *[Platforms] lure in consumers with “free” services but the cost is the collection of highly personal data to profit from and use of algorithms deciding what content they see* (The Australian 04/05/2018). While supporting measures to monitor digital platform activities, media companies also expressed concern over ACCC recommendations of an increased role for government in stipulating how media works.

While Google showed some support for regulation by welcoming the ACCC inquiry, it asserted that the existing regulations were sufficient:

...Google considers the existing unfair contracts regime, and the related protections in the Australian Consumer Law to be working effectively for consumers and businesses (Google submission 20/04/2018).

In addition to legitimizing their own practices, digital platforms highlighted the difficulty in regulating how they display content due to constant changes to their algorithms. They also pointed to the absence of evidence of market power imbalances:

We make hundreds of changes to algorithms every week to ensure that a person’s News Feed does the best job of connecting people with content that they will consider to be relevant and important, and also to ensure that the platform is a safe place for people to interact—we use algorithms to detect spam, fake accounts and content that breaches our Community Standards. The changes that we make to our algorithms are about innovation and learning from experience—the very things that competition laws and policy are intended to foster...This is not evidence of an imbalance of bargaining power. It is evidence of a focus on providing the greatest possible value to users (Facebook submission 18/04/2018).

Based on the results of the inquiry, the ACCC determined that Google and Facebook have substantial market power and maintained that this power is unlikely to erode in the short-to-medium term. Having substantial market power is not in itself prohibited by Australian law but as stated in the report, “*a firm with substantial market power could damage the competitive process by preventing or deterring rivals, including potential rivals, from competing on their merits*”. Based on the information presented by the ACCC, the government agreed that there is significant potential for self-preferencing by Google and Facebook to substantially lessen competition:

...Google and Facebook — their business model is based on creating a platform that they make enormous economic value from but they take no responsibility for what happens on there (The Australian 27/07/2019).

The government advocated the need for *policing*, which directly threatens a digital platform's ability to determine content algorithmically based on the data they collect. Once regulatory outcomes were suggested, digital platforms responded by successfully lobbying the ACCC and the government to revert to the voluntary code.

In December 2019, the government decided to delay mandatory action and instead allow voluntary adoption of codes of conduct. The ACCC issued a written request to the local chief executives of Google and Facebook to advise on the broad subjects for negotiation: *"Google and Facebook need a deal with publishers on the use of their content or face further regulation by the federal government"* (ACCC webpage 05/02/2019). Digital platforms were given several months to negotiate with media companies.

In April 2020, the ACCC provided a progress report indicating that the core issue of payment for content was highly unlikely to be resolved through this voluntary process. Following lack of progress from the digital platforms and absence of deals with media companies, the government decided to reverse their decision and instead proposed a mandatory bargaining code:

The platforms' unfair and monopolistic behaviors extend beyond simple loss of revenue and the mandatory code the ACCC will put in place will include, among other things, fair arrangements for access to data, understanding of algorithms...and fair treatment of news organizations' unique and valuable content (The Australian 15/05/2020).

As ACCC chairman Rod Sims highlighted, the days of the *"'trust us' response from Google and Facebook were over, saying the companies needed to take responsibility for what ended up on their platforms..."* (The Australian 11/12/2019).

The ACCC was commissioned to draft the new code. To this end a concept paper was released in May 2020, and feedback was sought on issues to be covered in a mandatory code. Google and Facebook both replied to the inquiry clarifying what would be considered news or a significant algorithm change and offering explanations of why some of the propositions were not workable on their side. Australia's media and industry commentators supported the ACCC's mandatory draft code for negotiation between media companies and digital platforms, with its aim to restore the balance of power between new and old media. In this negotiation round, the government moved from maintaining to creating institutions.

4.1.4 Algorithmic control of news media content – regulation (2020 – 2021)

In July 2020, the ACCC released a first draft of the new bargaining code and invited further submissions (*advocacy*). Google and Facebook responded critically, *undermining assumptions and beliefs* and rejected the code, claiming that it was unworkable and a threat to their services: “the law would break its [Google’s] search engine; undermine the concept of free internet, misunderstood how Google’s search engine works and is unworkable in the current form” (The Australian 13/03/2019).

Google added disclaimers on its YouTube and Google services warning that the new regulation would hurt provision of free services for consumers: “The way Aussies search every day on Google is at risk from new regulation” (Google landing page 3/12/2019). Facebook’s local CEO, Will Easton described the proposed law as “unprecedented in its reach” (Facebook submission 18/04/2018) as it sought to regulate every aspect of how the two tech companies did business with news publishers. He accused the ACCC of “misunderstanding the dynamic of the internet” (The Australian 01/09/2020). At the last minute, Google and Facebook lobbied fiercely for favorable amendments to the code, pushing back the timeline for the necessary legislation and *undermining assumptions and beliefs* that the proposed code was based on. They also threatened further consequences: Google announced it could halt its business in the Australian market and Facebook said it would block Australian users from sharing news on its digital platform and withdraw Facebook’s news services in Australia if forced to pay publishers fairly.

4.1.5 Algorithmic control of news media content – regulatory outcome

With the introduction of the bargaining code and the filing of enforcement cases against Google in court, the Australian Government’s institutional practices moved to *policing*. Despite pressure from Google and Facebook, the Australian Government did not change the main principles of how the code would function: namely that an amendment to the *Competition and Consumer Act 2010* would establish a mandatory code of conduct that applies to news media businesses and digital platform corporations when bargaining in relation to news content made available by digital platform services. Once designated by the government, digital platforms are obliged to enter into good faith negotiations with news publishers and have one month to reach a deal. If no deal is reached, a compulsory final offer arbitration process kicks in.

4.2 Case 2: Algorithmic control of extremist and terrorist content

In the decade prior to 2015, the rise of extremist and terrorist content and recruitment on social media made countering it a national counter-terrorism strategy priority in Australia.

4.2.1 Algorithmic control of extremist and terrorist content – discourse initiation (2015)

The discourse was initiated and driven by the AGD following concern that terror events could indicate a weakening of the state as a protective institution for its citizens. The government engaged in institutional work to maintain national security. It started by thwarting threats to existing institutions, expressing concern that digital platforms are not adequately monitored for extremist and terrorist content. After reviewing Australia's capacity for countering violent extremism (CVE) on social media, the AGD concluded that the necessary social media expertise was lacking and that *"some of this capability can be outsourced"* (AGD 01/01/2015), thus assigning responsibility to social media platforms to ensure national security and safety:

Social media platforms play an important role in identifying and acting on online extremist content. For example, companies such as Facebook and Twitter are actively monitoring, reporting and in some cases closing down violent extremist sites (Australia's CT Strategy, 2015).

4.2.2 Algorithmic control of extremist and terrorist content – discourse anchoring (2015 – 2017)

Several actors put forward their view on an appropriate form of control, basing the legitimacy of their view on different institutions.

The AGD *advocated* for political support by aligning with Five Eyes members for a coordinated, global response to ensure national security and fight extremist and terrorist content on social media. This discourse was anchored in practices of *constructing intergovernmental and industry normative networks* to establish collaboration for CVE between governments and social media platforms. Responsibility for CVE implementation was assigned to digital platforms, sanctioned by the Five Eyes alliance: *"there must be a sustained and aggressive approach to address these challenges"* (Five-Country Ministerial 27/06/2015).

Social media platforms aligned with the need to address extremist and terrorist content on social media and *embedded* the normative foundations into their platforms as both "free" and "safe": *"Our goal is to give people a place to share and connect freely and openly, in a safe and secure environment"* (Facebook 15/03/2015). They *routinized* CVE in removal practices involving user requests that were then processed by algorithms or humans. To legitimize their effectiveness, the social media platforms then reported content removal: *"We've suspended over 125,000 accounts for threatening or promoting terrorist acts, primarily related to ISIS"* (Twitter in The Australian 17/06/2016). In 2016, Facebook, Microsoft, Twitter and YouTube developed collaborative practices to identify and remove terrorist content:

Our companies will begin sharing hashes of the most extreme and egregious terrorist images and videos we have removed from our services – content most likely to violate all of our respective companies’ content policies (Facebook 05/12/2016).

The discourse was taken up by the media who largely *advocated* governmental action and gave voice to civil society (e.g., victims of terror attacks, academics, insiders). These voices were critical towards self-regulation of platforms, accusing them of abdicating responsibility and criticizing algorithmic content moderation systems as insufficient. For example, a victim’s father accused platforms of “*knowingly permit(ing) the terrorist group ISIS to use their social networks*” (The Australian 17/06/2016). A former Facebook employee asserted that “*(Algorithms) don’t have the ability to reason ... Artificial intelligence hasn’t gotten to the point where it can ... really function like a human brain and determine what has news value, what is good for the public, what is not.*” (The Australian 11/04/2017). Radicalization experts from academia discussed algorithms’ current inability to combine the institutions of free expression and national security using examples of misapplication, i.e. where false or exaggerated censorship harmed free press and where terrorist content remained undetected and was broadcast. Together, these actions represent the normative work of the media and civil society by *valorizing* governmental practices that maintain national security and *demonizing* the practices of social media platforms that break with social norms.

4.2.3 *Algorithmic control of extremist and terrorist content – discourse legitimization (2017 – 2019)*

In 2017, after the London Bridge and other terror attacks worldwide, pressure increased from government and media for digital platforms to provide more efficient measures against terrorism on social media.

The G7 and G20 together imposed normative sanctions on digital platforms. This bolster the institutional work of Five Eyes aimed at maintaining national security and creating normative networks. As a result, governments expanded their institutional power: the Australian prime minister Malcolm Turnbull declared a willingness to “*hold Facebook and other internet giants more accountable by law*” (The Australian 26/06/2017). Countering further content removal figures from digital platforms, the Australian home affairs minister Peter Dutton said, “*It is a significant figure but it may just be the tip of the iceberg in terms of the problem we need to deal with*” (The Australian 06/11/2018). British Prime Minister Theresa May “*took aim at companies like Google and Facebook for providing a ‘safe’ breeding ground for extremist ideologies*” (The Australian 20/06/2017). The German chancellor Angela Merkel put pressure

on social media platforms to “*act urgently to develop new tools to remove terrorist content*” (The Australian 26/06/2017). These statements show how government representatives took a stronger stance on monitoring extremist and terrorist content and threatened to hold digital platforms accountable through law.

Facing increased criticism of their practices, social media platforms doubled down on their self-regulating commitment to CVE. They announced the deployment of additional resources to train AI-algorithms to improve automated removal and for human oversight to complement algorithms when judging whether content was “*informative news reporting (...) or glorification of violence*” (The Australian 20/06/2017). In cases where the classification of content was unclear, digital platforms announced such content would be marked with a banner and excluded from marketing: “*We think this strikes the right balance between free expression and access to information without promoting extremely offensive viewpoints.*” (The Australian 26/06/2017). To strengthen the legitimacy of their measures, digital platforms reported on content removal figures: “*99 per cent of the content [removed] before being flagged by Facebook users*” (The Australian 30/11/2017).

The institutional pressure on social media platforms also led Facebook, Microsoft, Twitter, and YouTube to establish the Global Internet Forum to Counter Terrorism (GIFCT) to solidify and foster the joint work of “*representatives from the tech industry, government and non-governmental organizations*” (Facebook 26/06/2017). Internationally governments set the framework for the GIFCT by foregrounding the development of AI-algorithms (“*technological tools for automated detection and removal*”) to improve detection and removal of violent content (“*within 1-2 hours of upload*”), as illustrated by the following excerpt:

We call upon Internet companies to enhance the potential of the Database of Hashing to share hashes of known terrorist content across companies. We underscore the challenge to industry and we urge it to work collaboratively through the Global Internet Forum, to develop solutions to identify and remove terrorist content within 1-2 hours of upload, to the extent it is technically feasible, without compromising human rights and fundamental freedoms. We also urge the companies to pursue the development of technological tools for automated detection and removal (G7 19/10/2017).

The media valorized normative pressure and sanctions that governments exerted on the digital platforms, and further demonized insufficient CVE efforts from platforms, reporting overlooked terrorist videos and problems with software and human oversight. The media further promoted regulatory tendencies, stating that digital platforms risked “*a severe government*

intervention, including fines, unless they are willing to make their platforms a no-go zone for extremists” (The Australian 06/06/2017). This was supported by voices from academia calling for regulation: key actors emphasized for instance that “the reluctance to regulate meant platforms could continue getting away with big profits and little accountability....We have to ensure that we have the right rules in place to protect the public.” (The Australian 06/11/2018).

4.2.4 Algorithmic control of extremist and terrorist content – regulation (2019)

In March 2019, a mass shooting terror attack in Christchurch (New Zealand) was live streamed on YouTube and Facebook, with recordings subsequently circulated on the internet. This brought to light the inadequacy of YouTube and Facebook’s AI algorithms to remove violent live streams. The Australian prime minister announced talks with social media companies following the event, aiming to hold them more accountable:

The time has come for those who own and manage platforms to accept a greater responsibility for how they are used. A best-endeavours approach is no longer good enough. It’s clear that while social media companies have cooperated with authorities to remove some of that disgusting content, more needs to be done. If they won’t act, we need to (The Australian 20/03/2019).

Following talks with social media platforms, the Australian Government changed its stance from normative to regulatory work and introduced a new regulation that they justified as a consequence of the unwillingness of social media companies to take responsibility (Germany and the UK also switched to regulatory work). Rather than further negotiation towards a “regulatory bargain” with social media platforms, the government opted to impose regulations that made them fully accountable for the content on their digital platforms.

It was clear from our discussions last week with social media companies, particularly Facebook, that there was no recognition of the need for them to act urgently to protect their own users from the horror of the live streaming of the Christchurch massacre and other violent crimes and so the Morrison Government has taken action with this legislation (AGD 04/04/2019).

Social media platforms responded by once again raising the relationship between internet regulation and freedom of speech. They emphasized their practical legitimacy (“products are woven deeply into millions of businesses and billions of daily lives”), as in the following statement by Facebook:

New rules for the internet should protect society from harm while also supporting innovation, the digital economy and freedom of speech (...) These are complex issues to get right. How to police internet content is one of several topics in a broader debate over how governments should exercise control over platform companies whose products are woven deeply into millions of businesses and billions of daily lives (The Australian 09/04/2019).

4.2.5 Algorithmic control of extremist and terrorist content – regulatory outcome

On April 6, 2019, the Australian Government passed an amendment to the Criminal Code requiring social media platforms to expeditiously remove “abhorrent violent material”. This was defined as “records or streams of abhorrent violent conduct that reasonable persons would regard as being offensive” (s. 474.31), such as terrorist acts, murder, torture or rape (s. 474.32). The offense attracts fines of up to \$10.5 million or 10% of the annual turnover of a body corporate.

5 Discussion

Our findings provide novel insights into the regulation of algorithmic control (e.g., Khan et al., 2021; Riemer and Peter, 2021) by showing how institutional tussles between stakeholders to legitimize or delegitimize such forms of control shape both the process and outcome of regulation. In the following sections, we articulate a model that captures pluralistic institutional work for regulating algorithmic control and outline our contributions to the literature.

5.1 The process of institutional work for regulation of algorithmic control

Based on our findings, Figure 1 articulates the “process of pluralistic institutional work in regulating algorithmic control” (see Figure 1). As shown in our model, when concerns arose around the use of algorithms by digital platforms, the government with support from media and other stakeholders, initiated the process of regulation development (the grey left-hand-side box). Shaped by multiple institutions and the institutional work of multiple actors, the process evolved in three phases: (1) allocating responsibility; (2) governments using the threat of regulation to push digital platforms to self-regulate; and (3) negotiation around the scope of regulation (as shown in the three central boxes). We depict how the process accounts for multiple institutions, and how it shifts from establishing voluntary measures/self-regulatory measures to establishing mandatory/regulatory measures (as indicated by the two boxes in the background) until the final regulatory measure is set (the grey right hand side box).

Insert Figure 1

(1) *Allocating responsibilities.* The growing use of algorithms has triggered discussion on new and unforeseen responsibilities for platforms initially built on the institutions of free speech and free market, but which now come into conflict with other institutions (Bellanova and de Goede, 2022; Rauf, 2021). When use of algorithms by platforms is contested, governments engage in collaborative institutional work to compensate for their own lack of expertise in regulating algorithms by summoning the external expertise of stakeholders and platforms; for instance, by defining, advocating and constructing normative networks (Stewart et al., 2006), seeking expert feedback (case 1), and forging new intergovernmental and industry collaboration (case 2).

Platforms initially support the government's institutional work in anticipation of government regulation (Cusumano et al., 2021) and seize the regulatory process as an opportunity to strengthen their practical legitimacy. This occurs for example through engagement in the public inquiry process where they present their use of algorithms as support of free market competition (case 1). Or when they use algorithms for self-regulation to detect extremist and terrorist content (case 2). In this way, platforms embrace multiple existing institutions, but uphold and prioritize (Pache and Santos, 2010) the institutions they are built on.

Different stakeholders shape the discourse by valorizing government action to regulate algorithms and evidencing how platform practices harmed businesses or society. Their participation varies based on the discourse focus: when the discourse is economic in nature, it involves incumbent firms and experts addressing issues of market power imbalances, tackling antitrust issues, and looking to create an even playing field between businesses (case 1). Alternatively, when the discourse is societal in nature, it involves governments and media giving voice to civil society at the international level when addressing issues of national security (case 2).

(2) *Threat of regulation.* The controversial discourse on algorithmic control grows when regulatory gaps are revealed through the governmental inquiry process (case 1) or terrorist attacks (case 2). These gaps are attributed to self-interest and insufficient self-regulation on the part of digital platforms, and trigger discussion on the need for further regulation. As a result, governments take a tougher stance on inadequate self-regulation, tightening sanctions and publicly threatening to regulate digital platforms. In this phase, the institutional work changes from normative work to opting for regulatory work. Stakeholders, such as incumbent firms (case 1) or civil society (case 2), uphold established institutions, question the legitimacy of algorithmic control, and argue for the need to sanction misconduct by digital platforms. This

pushes governments to challenge the efficacy of platform self-regulation and develop regulation.

Digital platforms respond by defending their established practices and rejecting additional proposed regulatory measures. Rather than admitting this up front, digital platforms play up the advantages they bring in terms of innovation in the media market (case 1) and formalization of collaborative CVE practices (case 2), blurring the problem of accommodating multiple institutions. This shows that the synergy between existing institutions (e.g., free markets, free expression) and digital platforms is distorted when algorithms are built to prioritize economic goals that may in turn relegate other institutions (Riemer and Peter, 2021).

(3) *Negotiating regulation scope.* Digital platforms engage more actively in the regulation process once the government transitions from mainly normative work to the regulatory work of policing and defining the new regulations in the aftermath of a critical turning point. In case 1, when the government publishes the first draft of its mandatory code, platforms lobby the government to maintain voluntary measures, claim that the code is unworkable, and even threaten to leave the Australian market. This represents an endogenous critical event. In case 2, the government opts for regulation after an exogenous critical event – the live streaming of a terror attack; only when the platforms fail to prevail and refuse further talks with government does the government move decisively to regulate.

In line with Cusumano et al. (2021) we find that when the threat of government regulation becomes real, platforms respond by shifting from supportive to defensive institutional work, delegitimizing regulatory efforts, and attempting to narrow the scope of regulation to limit the potential damage of new regulation to their algorithmic functioning and legitimacy.

5.2 Contribution to theory and implications for research on regulation of algorithmic control

Based on our findings and our process model of institutional work for regulation of algorithmic control, our study offers three main theoretical contributions (see Table 5).

Insert Table 5

(1) Processual dynamics of pluralistic institutional work in regulating algorithmic control:

Prior literature highlights difficulties in regulating algorithms because they are opaque and subject to fast technology development (Borelli, 2021; Bristows, 2018; Riemer and Peter, 2021). Building on past studies of technology regulation and institutional work (Boon et al., 2019; Fuenfschilling and Truffer, 2016; Perner and Skjølsvik, 2018), we study regulation of

algorithmic control through the lens of pluralistic institutional work. Digital platforms embody some institutions (e.g., free market, free competition) and overlook others (e.g., fair market competition, national security). Therefore the pluralistic institutional work lens helps us to delineate the positions that shape back-and-forth negotiations between stakeholders over legitimate forms of algorithmic control. More specifically, governments engage in institutional work to maintain institutions that are threatened by algorithmic control, so digital platforms need to account for pluralistic institutions. Digital platforms respond by protecting the core of their business model – algorithms – defending the institutions the algorithms are built upon, and covering up the negative consequences of the incompatibility of multiple institutions. Affected stakeholders support the regulation process by giving evidence that platforms are unable to account for pluralistic institutions.

Introducing pluralistic institutional work may inspire future studies on technology regulation to further unravel the dynamics of regulation discourses in light of stakeholder constellations and intentions. For example, future studies may compare and contrast regulation debates in Europe and the US, which represent different institutional contexts. In Europe, the DSA and the DMA were agreed in March 2022, with a shared focus on creating fair competition in digital markets (DMA) and protecting consumers through monitoring of extremist, terrorist and morally questionable content (DSA). In the US, regulations are still under development. Pluralistic institutional work studies may unravel the different dynamics underlying these processes.

(2) Contested nature of legitimate forms of algorithmic control by platforms and stakeholders: We further extend the literature on regulation of algorithmic control by highlighting its contested nature and the power dynamics underlying pluralistic institutional collisions. While the power positions of platforms have been discussed multiple times (e.g., Boon et al. 2019; Cusumano et al. 2021), their influence on regulation remains under-researched.

Our findings illustrate how platforms demonstrate power through practical legitimacy. Their practical legitimacy allows digital platforms to influence the process and regulatory outcome and protect self-interests during the regulation process. Specifically, platforms redefine their position, first supporting government actions, then publicly going against them when regulation threatens the core of their business model – the algorithms. As we saw in our cases, platforms pushed back regulation by claiming publicly that regulation was unworkable or destructive, and by threatening to leave the market. By the same token, government was a wily actor and drew on its authoritative power, legitimacy and expertise to challenge platforms. In this they were

supported and complemented by the stakeholders who participated in multiple rounds of regulatory discussion and public inquiry. These actors formed the normative networks of intergovernmental and industry collaboration that complemented the government's work and maintained the contestability of the discourse. Our study thus shows that positions are (re)constructed taking into account stakeholder action. This highlights the power of 'elite actors' (Boon et al., 2019; Riaz et al., 2011) and the political nature of institutional work.

Given their limited power to establish regulation, stakeholders such as the media, business, or civil society actors support the discourse and play out their public role to uphold and advance the process. Future research may take a more explicit critical stance on the role of power in regulation processes and the deficiencies that result from power asymmetries. For example, self-regulation of platforms is not monitored or enforced but rather trusted, and the deficiency of measures are only highlighted by critical events or critical voices from affected stakeholders. This stands in stark contrast to calls for deliberation in democratic structures (Habermas, 2018; Aragon-Correa et al., 2020).

(3) Regulatory outcomes: interplay of self-regulation and regulation: We contribute to the literature on regulation and self-regulation of algorithmic control (Berkowitz and Souchaud, 2019; Cusumano et al., 2021). Aragon-Correa et al. (2020) called for attention to the combined effects and synergies of regulation and self-regulation. Our study nuances this interplay by highlighting the tensions between governmental regulation and platform self-regulation.

We show how the regulation process resulted in platforms involving themselves in self-regulation based on normative rules established through the discourse. The transfer of some responsibility from governments to digital platforms leads to more self-regulation by platforms. However, it gives leeway to platforms to follow their own interests in the absence of a neutral body to support, evaluate and, if necessary, correct processes of self-regulation. Simultaneously, while industry collaborations and normative networks have provided lessons for regulators, platforms can play on that lack of experience to influence the process in their favor. In such instances, scholars have argued that self-regulation is more effective when combined with credible threats of government regulation since platforms will self-regulate to preempt governmental regulation (Cusumano et al., 2021; Kwoka and Valletti, 2021). However, the threat of government regulation led platforms to refuse further collaboration, representing a critical turning point towards governmental regulation.

Moreover, scholars have emphasized how a regulatory outcome may be blurred by lobbying from different stakeholders in the discourse in order to defend their interests and shape the

regulation accordingly (Aragon-Correa et al., 2020; Boon et al., 2019; Mikalef et al., 2021). The governmental regulations presented in our two cases target liability of platforms rather than accountability of algorithms. This is despite the original intent being to regulate algorithms, in line with calls for their greater transparency (Kim and Routledge, 2022; Taddeo and Floridi, 2018). The regulatory outcome represents a compromise (Mikalef et al., 2021). Future research may deepen the consequences of such (self-)regulatory compromises.

5.3 Conclusion

This research offers new insights into the institutional work of different actors in the development of regulation of algorithmic control. In the context of algorithms and digital platforms, debate continues as to whether and how to introduce new laws to regulate platforms, with EU regulations such as the DSA and DMA at the forefront and others to follow. The implementation of these regulations will raise further research questions: how will these laws be enforced in practice? How will they affect the business model and algorithms of digital platforms? How effectively will regulation address the underlying problems of market power imbalances, the effect on quality journalism, and broadcast of extremist and terrorist content?

Our study shows a way to examine regulation processes against the background of pluralistic institutional collisions. A limitation of our research is the focus on one regulatory setting. Future research could build on these findings by zooming out to the wider ~~collective~~ institutional work of governments and digital platforms globally. We hope that by offering these insights our research inspires further work to advance understanding of the complex process of regulating algorithmic control.

References

- Aragón-Correa, J. A., Marcus, A. A., & Vogel, D. (2020). The effects of mandatory and voluntary regulatory pressures on firms' environmental strategies: A review and recommendations for future research. *Academy of Management Annals*, 14(1), 339–365.
- Asatiani, A., Penttinen, E., Ruissalo, J., & Salovaara, A. (2020). Knowledge workers' reactions to a planned introduction of robotic process automation—Empirical evidence from an accounting firm. In *Information Systems Outsourcing* (pp. 413–452). Springer.
- ACCC (2018) Digital Platforms Inquiry. Preliminary report. *Australian Competition and Consumer Commission*.
- ACCC (2019) Digital Platforms Inquiry. Final Report. *Competition and Consumer Commission*.
- Bailey DE, Faraj S, Hinds PJ, et al. (2022) We are all theorists of technology now: A relational perspective on emerging technology and organizing. *Organization Science*, 33(1): 1–18.
- Bellanova, R., & de Goede, M. (2022). The algorithmic regulation of security: An infrastructural perspective. *Regulation & Governance*, 16(1), 102–118.
- Berkowitz, H., & Souchaud, A. (2019). (Self-) regulation of sharing economy platforms through partial meta-organizing. *Journal of Business Ethics*, 159(4), 961–976.
- Biggar, D., & Heimler, A. (2021). Digital platforms and the transactions cost approach to competition law. *Industrial and Corporate Change*, 30(5), 1230–1258.
- Boon, W. P., Spruit, K., & Frenken, K. (2019). Collective institutional work: The case of Airbnb in Amsterdam, London and New York. *Industry and Innovation*, 26(8), 898–919.
- Borelli, M. (2021). Social media corporations as actors of counter-terrorism. *New Media & Society*, 14614448211035120.
- Bristows. (2018). *Artificial Intelligence: Public Perception, Attitude and Trust*. Retrieved from London: <https://www.bristows.com/viewpoint/articles/artificial-intelligence-public-perception-attitude-and-trust/>
- Cecez-Kecmanovic, D. (2019). The resistible rise of the digital surveillance economy: A call for action. *Journal of Information Technology*, 34(1), 81–83.
- Chuan, C.-H., Tsai, W.-H. S., & Cho, S. Y. (2019). Framing artificial intelligence in American newspapers. *Proceedings of the 2019 AAAI/ACM Conference on AI, Ethics, and Society*, 339–344.
- Clarke, R. (2019). Risks inherent in the digital surveillance economy: A research agenda. *Journal of Information Technology*, 34(1), 59–80.
- Clegg SR, Hardy C, Lawrence TB, et al. (2006) *Sage Handbook of Organization Studies*. 2nd edition. London: Sage, pp. 215–254.
- Common, M. F. (2020). Fear the reaper: How content moderation rules are enforced on social media. *International Review of Law, Computers & Technology*, 34(2), 126–152.
- Council of Australian Governments, issuing body. & Australia, issuing body (2015) *Australia's Counter-Terrorism Strategy: strengthening our resilience 2015*. Canberra Commonwealth
- Creed, W. D., Langstraat, J. A., & Scully, M. A. (2002). A picture of the frame: Frame analysis as technique and as politics. *Organizational Research Methods*, 5(1), 34–55.

- Creed, W. E., Douglas, M. A. S., & John, R. (n.d.). Austin. 2002. Clothes make the person. *Organization Science*, 13(5), 475–496.
- Cukier, W., Ngwenyama, O., Bauer, R., & Middleton, C. (2009). A critical analysis of media discourse on information technology: Preliminary results of a proposed method for critical discourse analysis. *Information Systems Journal*, 19(2), 175–196.
- Cusumano, M. A., Gawer, A., & Yoffie, D. B. (2021). Can self-regulation save digital platforms? *Industrial and Corporate Change*, 30(5), 1259–1285.
- Eisenhardt, K. M. (1989). Building theories from case study research. *Academy of Management Review*, 14(4), 532–550.
- Eisenhardt, K. M., & Graebner, M. E. (2007). Theory building from cases: Opportunities and challenges. *Academy of Management Journal*, 50(1), 25–32.
- Fairclough, N. (1995). *Media Discourse: Voices*. London: Edward Arnold.
- Fast, E., & Horvitz, E. (2017). Long-term trends in the public perception of artificial intelligence. *Proceedings of the AAAI Conference on Artificial Intelligence*, 31(1).
- Fisher C, Lee JY, Park S, et al. (2018) *Digital News Report: Australia 2018*. News and Media Research Centre, University of Canberra. <http://www.canberra.edu.au/nmrc/digital-news-report-australia-2018>
- Friedland, R. (1991). Bringing society back in: Symbols, practices, and institutional contradictions. *The New Institutionalism in Organizational Analysis*, 232–263.
- Fuenfschilling, L., & Truffer, B. (2016). The interplay of institutions, actors and technologies in socio-technical systems—An analysis of transformations in the Australian urban water sector. *Technological Forecasting and Social Change*, 103, 298–312.
- Ganesh, B., & Bright, J. (2020). Countering extremists on social media: Challenges for strategic communication and content moderation. In *Policy & Internet* (Vol. 12, Issue 1, pp. 6–19). Wiley Online Library.
- Ghazawneh, A., & Henfridsson, O. (2012). *Balancing platform control and external contribution in third-party development: The boundary resources model*isj_406.
- Goodrick, E., & Reay, T. (2011). Constellations of institutional logics: Changes in the professional work of pharmacists. *Work and Occupations*, 38(3), 372–416.
- Gorwa, R., Binns, R., & Katzenbach, C. (2020). Algorithmic content moderation: Technical and political challenges in the automation of platform governance. *Big Data & Society*, 7(1), 2053951719897945.
- Gurkaynak, G., Yilmaz, I., & Haksever, G. (2016). Stifling artificial intelligence: Human perils. *Computer Law & Security Review*, 32(5), 749–758.
- Habermas, J. (2018). *Inclusion of the other: Studies in political theory*. John Wiley & Sons.
- Helberger, N., Pierson, J., & Poell, T. (2018). Governing online platforms: From contested to cooperative responsibility. *The Information Society*, 34(1), 1–14.
- Jenny, F. (2021). Competition law and digital ecosystems: Learning to walk before we run. *Industrial and Corporate Change*, 30(5), 1143–1167.
- Joutsenvirta, M., & Vaara, E. (2015). Legitimacy struggles and political corporate social responsibility in international settings: A comparative discursive analysis of a contested investment in Latin America. *Organization Studies*, 36(6), 741–777.

- Khan, A., Brohman, K., & Addas, S. (2021). The anatomy of ‘fake news’: Studying false messages as digital objects. *Journal of Information Technology*, 02683962211037693.
- Kim, T. W., & Routledge, B. R. (2022). Why a right to an explanation of algorithmic decision-making should exist: A trust-based approach. *Business Ethics Quarterly*, 32(1), 75–102.
- Kira, B., Sinha, V., & Srinivasan, S. (2021). Regulating digital ecosystems: Bridging the gap between competition policy and data protection. *Industrial and Corporate Change*, 30(5), 1337–1360.
- Klausen, J. (2015). Tweeting the Jihad: Social media networks of Western foreign fighters in Syria and Iraq. *Studies in Conflict & Terrorism*, 38(1), 1–22.
- Kraatz, M. S., & Block, E. S. (2008). Organizational implications of institutional pluralism. *The Sage Handbook of Organizational Institutionalism*, 840, 243–275.
- Kwoka, J., & Valletti, T. (2021). Unscrambling the eggs: Breaking up consummated mergers and dominant firms. *Industrial and Corporate Change*, 30(5), 1286–1306.
- Lawrence, T. B., Leca, B., & Zilber, T. B. (2013). Institutional work: Current research, new directions and overlooked issues. *Organization Studies*, 34(8), 1023–1033.
- Leonard-Barton, D. (1990). A dual methodology for case studies: Synergistic use of a longitudinal single site with replicated multiple sites. *Organization Science*, 1(3), 248–266.
- Marjanovic, O., Cecez-Kecmanovic, D., & Vidgen, R. (2021). Algorithmic pollution: Making the invisible visible. *Journal of Information Technology*, 36(4), 391–408.
- Mikalef, P., Pateli, A., & van de Wetering, R. (2021). IT architecture flexibility and IT governance decentralisation as drivers of IT-enabled dynamic capabilities and competitive performance: The moderating effect of the external environment. *European Journal of Information Systems*, 30(5), 512–540.
- Möhlmann, M., Zalmanson, L., Henfridsson, O., & Gregory, R. W. (2021). Algorithmic management of work on online labor platforms: when matching meets control. *MIS Quarterly*, 45(4).
- Pache, A.-C., & Santos, F. (2010). When worlds collide: The internal dynamics of organizational responses to conflicting institutional demands. *Academy of Management Review*, 35(3), 455–476.
- Pandey, N., Dé, R., & Ravishankar, M. N. (2022). Improving the governance of information technology: Insights from the history of Internet governance. *Journal of Information Technology, Online first*: 02683962211054513.
- Parra, C. M., Gupta, M., & Mikalef, P. (2021). Information and communication technologies (ICT)-enabled severe moral communities and how the (Covid19) pandemic might bring new ones. *International Journal of Information Management*, 57, 102271.
- Patton, M. Q. (2002). Qualitative research and evaluation methods. Thousand Oaks. Cal.: Sage Publications, 4.
- Pemer, F., & Skjølsvik, T. (2018). Adopt or adapt? Unpacking the role of institutional work processes in the implementation of new regulations. *Journal of Public Administration Research and Theory*, 28(1), 138–154.
- Petit, N., & Teece, D. J. (2021). Innovating big tech firms and competition policy: Favoring dynamic over static competition. *Industrial and Corporate Change*, 30(5), 1168–1198.

- Pettigrew, A. (1990). Longitudinal field research on change: Theory and practice. *Organization science*, 1(3), 267-292.
- Rader, E., & Gray, R. (2015). Understanding user beliefs about algorithmic curation in the Facebook news feed. *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, 173–182.
- Rauf, A. A. (2021). New moralities for new media? Assessing the role of social media in acts of terror and providing points of deliberation for business ethics. *Journal of Business Ethics*, 170(2), 229–251.
- Reed, C. (2018). How should we regulate artificial intelligence? *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 376(2128), 20170360.
- Riaz, S., Buchanan, S., & Bapuji, H. (2011). Institutional work amidst the financial crisis: Emerging positions of elite actors. *Organization*, 18(2), 187–214.
- Riemer, K., & Peter, S. (2021). Algorithmic audiencing: Why we need to rethink free speech on social media. *Journal of Information Technology*, 36(4), 409–426.
- Rinfret, S. R., Scheberle, D., & Pautz, M. C. (2021). *Public policy: A concise introduction*. CQ Press.
- Rinta-Kahila, T., Someh, I., Gillespie, N., Indulska, M., & Gregor, S. (2021). Algorithmic decision-making and system destructiveness: A case of automatic debt recovery. *European Journal of Information Systems*, 1–26.
- Rowe, F., Ngwenyama, O., & Richet, J.-L. (2020). Contact-tracing apps and alienation in the age of COVID-19. *European Journal of Information Systems*, 29(5), 545–562.
- Slager, R., Gond, J.-P., & Moon, J. (2012). Standardization as institutional work: The regulatory power of a responsible investment standard. *Organization Studies*, 33(5–6), 763–790.
- Sun, S., Zhai, Y., Shen, B., & Chen, Y. (2020). Newspaper coverage of artificial intelligence: A perspective of emerging technologies. *Telematics and Informatics*, 53, 101433.
- Taddeo, M., & Floridi, L. (2018). How AI can be a force for good. *Science*, 361(6404), 751–752.
- UPI, 2021. Whistleblower: Facebook harms kids, stokes division, weakens democracy. URL: https://www.upi.com/Top_News/US/2021/10/05/facebook-senate-frances-haugen/8711633438623/
- Van Dijk, T. A. (1990). Social cognition and discourse. *Handbook of Language and Social Psychology*, 163–183.
- Weimann, G. (2000). *Communicating unreality: Modern media and the reconstruction of reality*. Sage Publications.
- Weimann, G. (2014). *New terrorism and new media* (Vol. 2). Commons Lab of the Woodrow Wilson International Center for Scholars.
- Whittaker, J., Looney, S., Reed, A., & Votta, F. (2021). Recommender systems and the amplification of extremist content. *Internet Policy Review*, 10(2), 1–29.
- Yin, R. K. (2014). Case study research: Design and methods. Fifth edit. *United States of America*.
- Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, 30(1), 75–89.

Tables

Table 1. Form of institutional work (Lawrence and Suddaby, 2006).

Forms of institutional work	Institutional foundation		
	Regulatory	Normative	Cultural-cognitive
Maintaining	<i>Enabling work</i> - The creation of rules that facilitate, supplement and support institutions, such as the creation of authorizing agents or diverting resources	<i>Valorizing and demonizing</i> - Providing for public consumption positive and negative examples that illustrate the normative foundations of an institution	<i>Embedding and routinizing</i> - Actively infusing the normative foundations of an institution into the participants' day-to-day routines and organizational practice
	<i>Policing</i> - Ensuring compliance through enforcement, auditing and monitoring	<i>Mythologizing</i> - Preserving the normative underpinnings of an institution by creating and sustaining myths regarding its history	
	<i>Deterring</i> - Establishing coercive barriers to institutional change		
Creating	<i>Advocacy</i> - The mobilization of political and regulatory support through direct and deliberate techniques of social suasion	<i>Constructing identities</i> - Defining the relationship between an actor and the field in which that actor operates	<i>Mimicry</i> - Associating new practices with existing sets of taken-for-granted practices, technologies and rules in order to ease adoption
	<i>Defining</i> - The construction of rule systems within a field that confer status or identity, define boundaries of membership, or create status hierarchies	<i>Changing normative associations</i> - Re-making the connections between sets of practices and the moral and cultural foundations of those practices	<i>Theorizing</i> - The development and specification of abstract categories and the elaboration of chains of cause and effect
	<i>Vesting</i> - The creation of rule structures that confer property rights	<i>Constructing normative networks</i> - Construction of interorganizational connections by which practices become normatively sanctioned and that form the relevant peer group with respect to compliance, monitoring and evaluation	<i>Educating</i> - The educating of actors in the skills and knowledge necessary to support the new institution
Disrupting	<i>Disconnecting sanctions</i> - Working through state apparatuses to disconnect rewards and sanctions from some set of practices, technologies or rules	<i>Dissociating moral foundations</i> - Disassociating the practice, rule or technology from its appropriate moral foundation within a specific cultural context	<i>Undermining assumptions and beliefs</i> - Decreasing the perceived risks of innovation and differentiation by undermining core assumptions and beliefs

Table 2. Data sources and types.

	<i>Type</i>	<i>Total</i>
Case context data		410 articles
Media articles	The Australian 2015–2022	410 articles
Case data: case 1		204 articles 339 documents
Media articles	The Australian 2017–2022	204 articles
Policy and industry submission documents	Regulatory documents and government reports Submissions commissioned by ACCC ACCC industry events Submissions to inquiry 2018 Submissions to inquiry 2019 Submissions to the concept paper on the Mandatory Code, July 2020 Submissions to Mandatory Code draft, December 2020	8 documents 5 reports 8 reports 78 submissions 124 submissions 43 submissions 73 submissions
Case data: case 2		65 articles 144 documents
Media articles	The Australian 2015–2019	65 articles
Policy documents	AGD publications	55 documents
Industry documents	Digital platform publications	89 documents

Table 3. Data structure case 1: Algorithmic control of news media content.

	Initiation (2017 – 2018)	Anchoring (2018 – 2019)	Legitimation (2019 – 2020)	Regulation (2020)
Problem definition	Concerns about extensive power of digital platforms, media companies, and advertisers	Evidence from the public inquiry of market power imbalances	Lack of action from digital platforms despite a normative framework to negotiate fair deals with media companies	Threats from Google and Facebook to limit their services in Australia if code becomes law
Main stakeholders	Government, ACCC; digital platforms; media, industry, academia, civil society			
Institutional work				
<i>Government, ACCC</i>	Thwarting threats; defining and enabling work; constructing responsibilities	Advocating; constructing normative networks	Advocating for policing; defining rules and vesting; tightening sanctions	Transition to policing; enabling work; defining the new regulation
<i>Digital platforms</i>		Aligning; joining normative networks; routinizing and embedding	Legitimizing self-regulatory measures; undermining assumptions, beliefs; mimicry, education	Resisting; defining further aspects of the code to protect their own practices
<i>Media, industry</i>	Advocating for inquiry	Advocating; providing evidence; valorizing and demonizing	Advocating; providing evidence; valorizing and demonizing	Advocating; providing evidence; valorizing and demonizing
Solution orientation/action	Normative: problem inquiry	Normative: government to push negotiations for fair deals between platforms and media	Normative to regulatory: government to suggest mandatory code	Regulatory: government introduces the bill and its amendments
Key events	ACCC to conduct an inquiry into digital platforms	February 2018: ACCC released a paper seeking feedback on issues. 70+ submissions were received between February to April, 2018. ACCC released preliminary report in December 2018	ACCC DPI Final report. ACCC conducted a series of events to inform the inquiry from January to March 2019. April, 2020: ACCC to develop a mandatory code	May, 2020: ACCC releases a draft version of the news media bargaining code. May to June, 2020: ACCC launches consultation period. August, 2020: ACCC court filing. September 2020: Google and Facebook threaten consequences

Table 4. Data structure case 2: Algorithmic control of extremist and terrorist content.

Phase	Initiation (2015)	Anchoring (2015 –2017)	Legitimation (2017 – 2019)	Regulation (2019)
Problem definition	Digital platforms criticized for allowing extremist and terrorist content on their platforms; lack of governance mechanisms	Governments and digital platforms to collaborate on CVE, leveraging algorithms for content removal	Pressure on digital platforms to improve measures after new terrorist attacks (e.g., London bridge 03/07/2017)	Christchurch event revealed that measures by digital platforms were insufficient and inadequate to stop live streaming of such events
Main stakeholders	Government (AUS, international), AGD; digital platforms; media, civil society			
Institutional work				
<i>Government (AUS, international), AGD</i>	Thwarting threats; defining; constructing responsibilities	Advocating; constructing normative networks	Advocating; tightening sanctions; threatening regulation	Policing; defining regulation
<i>Digital platforms</i>		Joining normative networks; routinizing and embedding	Formalizing normative networks; routinizing and embedding	Legitimizing self-regulation; rejecting regulation
<i>Media, civil society</i>		Valorizing and demonizing	Valorizing and demonizing	Valorizing and demonizing
Solution orientation/action	Normative: government assigns responsibility to digital platforms and push self-regulation	Normative: government increases pressure for self-regulation	Normative to regulatory: government threatens regulation	Regulatory: government introduces regulation to complement insufficient self-regulation
Key events	Social media was put on the national agenda against terrorism; government emphasized the need for collaborative work with platforms	The Five Eyes intelligence alliance creates a normative network with platforms; digital platforms develop collaborative CVE practices (database for sharing hashes)	Worldwide terror attacks (Baghdad, London, Melbourne); G7 and G20 joined the normative network; the Global Internet Forum to Counter Terrorism (GIFCT) was founded	Christchurch terrorist attack streamed live on Facebook and YouTube; amendment to Australian Criminal Code

Table 5. Overview of contributions

Contributions	Key claims
(1) Processual dynamics of pluralistic institutional work for regulating algorithmic control	Stakeholders engage in pluralistic institutional work to create, maintain and combine institutions as algorithmic control by digital platforms embodies some institutions and overlooks others.
(2) Contested nature of algorithmic control	Pluralistic institutional collisions occur when power dynamics shift between platforms enacting their practical legitimacy and governments enacting their authoritative power
(3) Regulatory outcomes: interplay of self-regulation and regulation	The regulatory outcome embodies tensions between government regulation and platform self-regulation

Figures

Figure 1. Process of pluralistic institutional work in regulating algorithmic control.

