

Governing trust in European platform societies: Introduction to the special issue

European Journal of Communication
2021, Vol. 36(4) 323–333
© The Author(s) 2021



Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/02673231211028378
journals.sagepub.com/home/ejc



José van Dijck

Utrecht University, The Netherlands

Introduction

For the past 20 years, digital platforms have created enormous wealth for companies and convenient benefits for users as they enabled global online connections. But they have also generated a variety of problems for users and societies: an avalanche of misinformation, disinformation and fake news has infused the public sphere; hate speech and trolling, along with conspiracy theories, have flooded the Internet, deeply impacting the social fabric of democratic societies; privacy scandals and security leaks contributed to widespread distrust of platforms, triggered particularly by the Facebook–Cambridge Analytica scandal in 2016 that disclosed practices of online election intervention. American big tech companies are frequently accused of tax evasion and undermining labour laws. In late 2020, four of the Big Five tech companies were taken to court on allegations of competition fraud and antitrust violations, in both the United States and Europe. And in February of 2021, both Google and Facebook clashed with the Australian government about a new law requiring these companies to pay publishers for their links to original news content. The so-called ‘tech-lash’ against platforms culminated in a series of claims revealing a lack of trust in their ability to govern the technological systems that underpin many societal structures (Van Dijck, 2019).

Behind such profound distrust is the realization that long-standing public values promoting open, democratic societies – privacy, security, tolerance, fairness, equality, autonomy and so on – are compromised in an online world that is currently dominated by a few handfuls of American and Chinese tech companies. Evidently, in capitalist societies, public values have never prevailed over commercial values anyway, but the rise of platformization and datafication is posing new threats to these ideals. Since much of our

Corresponding author:

José van Dijck, Utrecht University, 3584 CS Utrecht, The Netherlands.

Email: j.f.t.m.vandijck@uu.nl

private and public communication has moved to online infrastructures, along with an increasing percentage of our social and economic activities, the issue of ‘trust and governance’ has taken centre stage. This special issue of the *European Journal of Communication* will address a few poignant questions in light of a changing media landscape: How can European societies ensure the durability and effectiveness of public values in an online world that is largely governed by global, corporate platforms? What are (old and new) mechanisms for establishing trust and trustworthiness in the context of online communication and digital platforms (Baghranian, 2019; O’Neill, 2020)? And how are public values conventionally anchored in trusted professional routines, legal frameworks, and institutional checks and balances, transferred to the digital realm? These are fundamental questions, raising a broad spectrum of issues that go well beyond the narrow academic frame of communication science.

Therefore, an interdisciplinary approach to this complex problem of governing public trust in platform societies is indispensable. Platformization and digitization are processes akin to industrialization or electrification. What is at stake here is nothing less than the restructuring of our communication infrastructure as part of a technical and economic overhaul of society against the backdrop of a shifting (geo)political world order. While this angle may be too broad for a single special issue, we will try at least to capture some of the pressing concerns with regard to the questions raised above. Taking a bird’s-eye perspective, we will discuss how to govern platform societies, promoting public values and establishing trust in democratic institutions that have become dependent on global digital infrastructures. In this introduction, we will probe the three main ingredients of its central theme ‘Governing trust in European platform societies’.

First, we will tackle the concept of *platform societies* and the layered ecosystems they have come to rely on. Second, we explore how platform technologies have introduced a new corporate-computational model of trust. Online environments are increasingly *governed by* automated mechanisms of selection and distribution – mostly self-regulated by tech companies – while the *governance of* platforms still largely escapes the control of governments, institutions and users who demand public accountability. And third, we situate the dependence of *European societies* on American (and to a lesser extent Chinese) global platform ecosystems in a rapidly shifting geopolitical world order.

Our object of scholarship is a moving target in more than one way. Platform ecologies do not stop at national borders; their technological wrappings are constantly changing, and they do not let themselves be caught by a single academic (or regulatory) framework. Notwithstanding these fluid boundaries, this introduction will try to highlight how the six articles in this special EJC-issue address some of the pressing concerns regarding platforms and trust in their governance.

Platform societies

The subject of this special issue finds its roots in the growing importance of online platforms, defined as ‘programmable architectures designed to organize interactions between users online’ in our daily lives (Van Dijck et al., 2018: 9). Even though we have long considered multi-sided platforms to be neutral conduits of online interactions, their intricate dynamics are part and parcel of the political-economic systems through which they

have been adapted in societies across the globe. Online platforms are not simple technological products; they are enabled by hardware infrastructures, fuelled by data (often generated by users), automated and organized through algorithms, formalized through ownership relations and monetized via business models. Large amounts of data form the input of artificial intelligence (AI). Data-hungry machines and bots are increasingly used for automating human acts such as communicating, buying and decision-making. As a consequence, the mutual shaping of human and machine intelligence is a potential source of conflicting interests between the (commercial) goals of tech companies and the (public) interests of individual users, communities and societies. These conflicts of interests may divulge how the dynamics of the platform ecosystem have come to affect many of our daily practices, professional routines and institutional structures.

Let's take the widespread distribution of disinformation and misinformation through online channels as an example of the online ecosystem's complexity. Many have pointed at troll factories that produce and disseminate disinformation for commercial or political purposes, targeting susceptible users who are themselves deliberate or unwitting spreaders of falsehoods and propaganda. Social media channels such as YouTube, Twitter and Facebook have been accused of exploiting a computational infrastructure driven by business models that incentivize disinformation. And governments, along with tech companies, have been blamed for not taking sufficient measures to stop the widespread 'infodemic' of inaccurate health information at the time of the Covid-pandemic (Van Dijck and Alinejad, 2020). A recent EU-report identifies how disinformation arises from the perfect collusion of the attention economy and its business models, platforms' choice architectures, algorithmic content curation and a lack of public oversight or democratic governance (Lewandowsky et al., 2020).

Taking apart such a problem as disinformation, we have to analyse platform societies simultaneously as a *sociotechnical* and *political-economic* concept. Online platform ecosystems consist of various layers or 'stacks' of applications and services into a seamless whole (Van Dijck, 2020). Built upon a *digital* infrastructural layer of wires, cables, data centres, chips, protocols, hardware, software and a number of devices, platform services have gradually metamorphized into a *computational* infrastructure that supports all data-based and algorithmically steered interactions. The latter includes for instance cloud services for data storage, analytics and distribution; operating systems, search engines, social media networks, messaging services and identification services; app stores, advertising platforms, online marketplaces, maps and navigation services and a number of others. This move towards the 'infrastructuralization' of some online platforms has turned a small core of proprietary platforms into the essential gatekeepers to networked ecosystems (Plantin et al., 2018). There is not a single private or public sector in society that for its functioning is not at least partially dependent on this online infrastructure. News organization, health institutions, schools or mobility services – they all have major stakes in computational platforms that are now almost as crucial as public utilities such as electricity networks and water supplies. As argued by Jean-Christophe Plantin in his contribution to this EJC-issue, it should therefore not come as a surprise that questions of trust have shifted from sectors to infrastructures, from institutions to automated systems and from discourses on technical standardization to geopolitical discussions. We will return to Plantin's contribution in the last section of this introduction.

While digital infrastructures define the ‘deep architectures’ upon which computational services are built, it is important to understand *how* these architectures impact all kinds of services stacked on top of them. For one thing, platform technologies that are proprietary owned and operated often funnel data flows across their ‘walled gardens’ of integrated services. You are either caught in the Google-stream of services or wedged by the Apple-universe of hardware and software amenities. Once you’re inside the Facebook-universe (including WhatsApp, Instagram and Messenger), it is very hard to switch to other social media services without giant switching costs. The markets for crucial online services such as search, social networking, advertising, cloud services and app stores are typically dominated by one, two or at most a three of the Big Five tech companies, inevitably causing monopolies, duopolies or, more generally, ‘mologopolies’ (Petit, 2016; Smyrnaois, 2018). In recent years, the combined market power of the Big Five tech companies – Google, Apple, Facebook, Amazon, Microsoft (GAFAM) – has grown to unprecedented levels, reaching 20% of the American stock market’s total worth in 2020 (Eavis and Lohr, 2020).

Beyond the issue of market power, we are concerned with platform companies’ societal power, and more specifically, with the trustworthiness, reliability and transparency of the technological systems they exploit. Should we trust tech companies to design the blueprint of our digital infrastructures and allow them to develop and govern their own platform dynamics as long as they satisfy consumer expectations of convenience and free services? Or should citizens and governments require that all tech companies abide to standards such as openness and transparency to allow for fair competition and user control? As it stands now, tech companies are defining their own technical standards by which online infrastructures are ruled. For instance, Facebook and Google are the biggest operators of online platforms in advertising, news distribution and social networking; the intricate workings of their algorithmic ad auctions and personalization algorithms remain a well-kept business secret. By the same token, Google and Apple’s app stores form the ultimate gatekeepers to the distribution of consumer apps. To reach the mobile devices of millions of users, developers have to comply with the technical-economic conditions imposed by their app stores, often without the possibility of arbitrage or auditing the fairness of some rules. How do users, businesses, app developers and others know they can trust the platforms they have become heavily dependent upon?

Platform societies and shifting models of trust

Observing the recent evolution of platform ecosystems, we need to ask how epistemic trust is at the heart of a socio-technical and ideological power shift. Open, democratic societies are moving from an institutional-professional model of trust towards a computational-corporate model of trust. Whereas the first model is predicated on human-made rules of power governed by publicly accountable institutions and professional norms and routines, the second one is grounded in an obscure dynamic that mixes personalized data flows, algorithmic computation and proprietary business models. Let us return to the example of disinformation and the impact of platformization to illustrate this. The sector of communication and news has traditionally been governed by a high-trust framework anchored by institutional norms and professional routines – think of the editorial

selection process and news organizations' content liability. These conventional anchor points of trust have not been adopted in the low-trust Internet environment where news items are selected by commercially incentivized algorithms and where distribution is programmed by personalized data flows. Global tech companies have reconfigured citizen's access to the world of news and information, destabilizing legacy media's institutional autonomy and authority in the process, and yet they have refused to adopt the responsibilities and accountability that comes with societal institutions (Dutton and Dubois, 2015). As a corollary to this process, the quick rise of 'free' social networks with their personal ad-driven newsfeeds has seriously undercut the business models of traditional news print and journalism (Braun and Eklund, 2019).

The shift towards a computational-corporate model of trust is not restricted to just infrastructure or to just one specific sector, such as news and (mass) communication; it encompasses all private sectors *and* public institutions, including health and education. In addition, the gravitation from 'institutional' to 'computational' trust is not a given, but a hotly disputed transfer of power. Tech companies are increasingly trying to gain the public's trust in their systems by collaborating with governments and legacy institutions, particularly in their effort to distinguish accurate information from disinformation. For instance, in the fight against the infodemic following the Covid-19 pandemic, platforms like YouTube, Facebook and Twitter worked with the WHO and national governments to automatically direct online users to official information about treatment and vaccination. Aligning their interests with public institutions may help the tech companies to bolster trust in their platforms' authoritativeness. However, such alignments inherently raise questions of clashing private and public interests.

As Judith Simon and Gernot Rieder demonstrate in their contribution to this special issue, the domain of 'e-health' turned into a locus of contested trust with the recent development of the Corona-Warn-App in Germany in 2020. The conditions to foreground public values in the development of this app, such as protecting user privacy and allowing for democratic control, played out at various levels, from design to distribution. Questions of open standards surfaced when the app-development team weighed the benefits of centralized data systems versus decentralized protocols. And the dispute about the potential distribution of the Corona-app via the Apple App Store characterized the public's concern about the tracking and tracing of health data through proprietary platforms. Simon & Rieder's analysis of the debate discloses how public values are negotiated at all stages of design and development of technical systems, and these negotiations can hardly be understood without taking into account the architectures of evolving platform ecosystems. If the Corona-Warn-App design process in Germany showed anything, it may be a keen awareness of how institutional trust gets *distributed* between governments, institutions, technologies, its owners and users.

Platform societies do not naively transfer the governance of trust to new technical agents; the conditions for governing trust are actively negotiated between private (corporate, consumer), public (institutional, governmental) and civil society (NGOs, citizens) actors. They all play different roles in the mutual shaping of technology and society. Users – both as consumers and citizens – have a distinct part in this mutual shaping: by engaging themselves, they can exert power over their ultimate implementation in daily

practices. Far from being ‘victims’ or ‘puppets’ of technology, they can become active agents in its modelling.

Jo Pierson, in his contribution to this special issue, investigates this as a paradox where users feel compelled to appropriate socially indispensable apps in everyday life, while these apps subject them to the corporate control mechanisms that are hardly knowable. He investigates how built-in messaging apps (e.g. Facebook Messenger or the Apple messaging app) and autonomous messaging services (e.g. WhatsApp) have become distinctive channels for private online communication. Users ‘appropriate’ and ‘domesticate’ these services differently from social media apps such as Facebook or Instagram, which they consider to be public, mass-oriented channels. In doing so, they explore different positions of trust, not only towards other users but also towards the operators of these popular platform services. Users’ dependency on – and ‘blind’ trust in – the algorithmic processing of their communication data can be considered a sign of disempowerment; however, as Pierson argues, users can also stage their own interventions, for instance by exchanging one messenger app for another, hence empowering themselves as active co-creators of communicative practices. He deploys the strategy of ‘infrastructural inversion’ to explore the hidden or opaque affordances of these messaging services to explain how users can disclose the underlying (public and private) values in such systems.

Platform technologies are increasingly fuelled by AI systems that are often black boxed, so their operation is hidden from users’ view. As Alison Powell explores in her essay in this special issue, users can demand explanations of AI-systems to generate transparency and accountability. Automated systems, such as recommendation systems for news selection, are often too complex for users to understand; even designers may not have enough expertise to fully comprehend their precise operation. So the question raised in this article is whether the ‘explanation’ of algorithmic dynamics and decision-making can be turned into a condition of these systems’ governance. And is explanation alone enough to remedy the significant information asymmetry between the automated decision system and the individual user who might have a right to, or an interest in, an explanation? The more we rely on programmable infrastructures, the more poignant the question of ‘explanation’ and transparency becomes. Not just as a means to guarantee a private citizen’s trust in specific apps, but as a way of interrogating which *public* interests are at stake in AI-powered systems.

Trust in platforms and platform societies, in short, is the outcome of deliberation and negotiation. It is the result of individuals’ and collectives’ critical engagement with the new computational-corporate model of trust that is gradually inserted in the fabric of Western societies. These societies, which have long relied on institutional-professional anchors of trust, are gradually trying to find a new equilibrium – a balance that will be highly staked in the development of trusted platform governance.

Governing platforms

The growing dependency of citizens and public sectors on global proprietary platforms strongly impacts the ability of institutions and governments to run societies based on

democratic values. When the platform economy first began to take off around the year 2000, all eyes were fixated on values such as privacy, security and accuracy, emphasizing the interests of individual *consumers* and *markets* in datafied environments. However, as digital infrastructures started to penetrate deeper into the fabric of societal structures, concerns about *citizen's* interests and *collective* values, such as transparency, fairness, nondiscrimination and democratic control, were pushed to the fore (Van Dijck et al., 2019). Corporate platforms have gradually accrued the capacity to algorithmically demarcate fairness from discrimination, and tell accurate news from disinformation, without allowing anyone to look 'under the hood' of their processed data circuits. As gatekeepers to information and advertising channels, they send billions of people personalized news feeds every day, without offering any transparency about the algorithmic decisions that govern their automated selection processes. As Tarleton Gillespie (2010) has argued, we are increasingly governed *by* platforms whereas the governance *of* platforms has lagged behind.

It should, therefore, come as no surprise that public distrust of the new gatekeepers of information and communication channels has noticeably mounted. Tech companies came under intense scrutiny because their power to *govern* people's everyday online activities had grown disproportionate in relation to the societal institutions and governments that were supposed to govern *them* (Dolata and Schrape, 2018; Gillespie, 2018). Particularly since 2016, Facebook, YouTube and Twitter have received serious criticisms for their reluctance to clean up their social networks by filtering out hate speech and disinformation. Pressured by governments and advertisers, social media networks finally scaled up their algorithmic detection mechanisms; Facebook, for instance, claims its platform now automatically filters out over 95% of the messages containing hate speech and disinformation. However, European governments and citizen groups argue self-regulation is not enough to restore trust in platforms as our main distributors of reliable news and information (Gorwa et al., 2020).

Global online platforms have not (yet) gained the level of trust that institutions or governments used to have or still have in most Western-democratic countries (Duffy, 2018). Some platforms aspire to become institutional entities to gain higher levels of public trust, but they refuse to subject themselves to the accountability apparatuses that usually come along with such status. As Philip Napoli shows in his contribution to this special issue, the interdependency of news organizations and online gatekeepers is paradoxical, to say the least. On the one hand, traditional news organizations are dependent on Facebook, Google (YouTube) and Twitter for their distribution, monetization and visibility of new items; on the other hand, journalists and news organizations have to critically scrutinize the tech barons' powers. Examining the 'platform beat' of journalism as a double-edged sword, Napoli points out how the 'fourth estate' function of institutional journalism stands in tension with its own dependency on the algorithmic mechanisms built into the platform ecosystem. Can critical journalism enhance the accountability and trustworthiness of platforms? Or should governments step in to govern the 'unruly' and 'invisible' mechanisms of platforms?

Up until 2020, the major platform gatekeepers have managed to maximally exploit the minimal constraints that national governments have put on their ability to grow into

self-regulating ecologies. The grey area of legal permissiveness – a void legitimated by Section 230 of the Communications Decency Act in the United States and the Digital Market Directive in Europe – has been allowed to grow into a global loophole that helps tech companies to escape the governmental powers of national legal frameworks (Napoli, 2019). A persistent lack of government interference into online spaces has left the design of platform architectures and the control of algorithmic mechanisms almost entirely to the companies that own and operate them. Due to their exceptional legal status, they remain unscathed by institutional checks and balances or legal sanctions. The liberties of platforms transgress the boundaries of particular legal frameworks (e.g. privacy law, competition law) as well as the boundaries of national legislatures. Legal regimes commonly pertain either to public or private infrastructures or to specific sectoral responsibilities (e.g. in the news or health sector). In the case of platform ecologies, lawmakers and regulators are facing *all* these regulatory challenges *at the same time*.

Stefan Larsson, in his contribution to this special issue, raises the question of comprehensive governance of platforms through the lens of current competition regulation. He asks: ‘To what extent can the platforms’ own abilities to govern their infrastructures, that is, to be de facto regulators over both human behaviour and market circumstances, be seen as a challenge for contemporary competition regulation?’ Larsson observes that there is a strong relation between transparency and public trust in platforms. This is evident not only for news distribution and social media networks, but also for app markets, online retail, digital maps and so on. As noticed before, platforms such as Facebook, Google Search and YouTube, whose computational models govern the selection and moderation of content, are virtually impermeable due to a lack of external audits or formalized public scrutiny. Larsson argues that these platforms’ power to govern their own infrastructure as well as their automated handling of moderation, pricing and data processing poses significant challenges for regulatory authorities. Beyond these challenges, he points at Europe’s dependence on US platforms for vital and popular consumer services as well as the American creation of competitive commercial markets for communication and information services – the ‘marketplace of ideas’.

The incongruence between the transnational and transgressive sectoral powers of tech companies versus the limited scope of most legal frameworks indeed forces governments to look into expansive regulatory models to govern the tech giants. In doing so, they are inexorably confronted by the limiting scopes of national regulatory frameworks in the face of the Big Five’s global reign over the free flow of data across borders and boundaries. Therefore, the EU’s supra-national regulatory power may be the most effective level of tackling platform governance, especially when it comes to securing European public values such as privacy, democratic control and equal access. However, despite the ‘Brussels effect’ of recent regulation such as the General Data Protection Regulation (implemented in 2018) and the Digital Services and Digital Markets Act (proposed in 2020), the EU’s actual impact on platform governance remains inadequate (Bradford, 2020). Governing platform societies is inevitably a geopolitical affair that forces scholars to look at socio-technical systems through the lens of global political economies.

Europe between American and Chinese platform ecosystems

The third and last focus of this special issue is on European ways of governing platform societies in light of a gradually intensifying geopolitical contest between the United States and China. It is a contest to control the vital digital infrastructures of wires and cables as well as the computational infrastructure or platform ‘stacks’ built on top of them – the essential groundwork for processing large amounts of data flows distributed across platforms. Over the past two decades, two rivalling platform ecosystems have emerged that dominate the global exchange of data flows: the American GAFAM-system vis-à-vis the Chinese ecosystem, run by three giant platform operators Baidu, Alibaba and Tencent (BAT). Whereas American companies have shown to exert strong lobbying powers over American and European governments, the Chinese state has strict control over the BAT-companies’ data steering (Van Dijck, 2019). Putting aside for now these two ecosystems’ strongly interrelatedness, we look instead at Europe’s position in this geopolitical choreography.

Despite boasting a few handfuls of unicorns in the tech sector, Europe has no major platform ecosystem of its own; for their digital and computational infrastructures, European countries are largely dependent on the GAFAM-run ecosystem and, to a lesser degree, on the BAT-ecosystem. Alibaba is increasingly active in the European digital marketplace, as is its rival Amazon; app store distribution happens overwhelmingly via Google and Apple. Microsoft, Facebook and Amazon all have major stakes in data centres built on European soil, but the cloud services owned and operated in these centres are overwhelmingly American. Europe’s dependence on American big tech, besides divulging its infrastructural vulnerability, has become a geo-political liability, as it is now caught between the superpowers’ fight over technological control. Indeed, the EU is a supra-national body which, due to the size of its common market, can theoretically exert substantial influence over its ‘system rivals’. But considering the unequal distribution of tech power, it is fair to ask: How can European states ensure the implementation of public values in their own platform societies when the technical systems on which they depend are owned and operated overwhelmingly by non-European corporations, controlled and regulated by American and Chinese authorities?

Jean-Christophe Plantin addresses this question in his contribution to this special EJC-issue, first of all by warning that the very concept of ‘public values’ may not even mean the same thing in different ideological contexts. His article shows how the polysemy of the terms ‘open’ and ‘transparent’ have become the very stakes in a geopolitical fight about infrastructural standards. Plantin describes the case of ‘open radio access network’ (RAN for short): an open-source version of radio access equipment which is a key component of future 5G infrastructure.

For advocates of such an open-source model of the RAN, the terms modularity and openness are emancipatory notions referring to operators gaining deeper control of their own infrastructure. The American government, however, deployed the principle of ‘openness’ to create an opposition between its own ‘trusted’ open telecommunication systems and the presumed ‘untrustworthy’ Chinese systems of blackboxed technologies, directly targeting Huawei. In the EU – home to the two other major equipment manufacturers for RAN technology, that is, Ericsson and Nokia – another meaning of ‘open’ prevailed, as

Plantin argues: ‘The EU industrial policy favours open competition between various standards without direct intervention through state subsidies and national mandates’, at the opposite of the direct subsidies provided – ironically enough – by both China with Huawei and the United States with open RAN. In other words, when technical standards deployed to solidify trust (e.g. open standards, modularity, interoperability) are negotiated in geopolitical discussions about the Internet’s governance, their meaning becomes contested and imbued with ideological and political interests.

Conclusion

European platform societies are not doomed to fall prey to either American or Chinese domination of a new geopolitical world order. It is more likely that through an increasing awareness of its own priorities in terms of public values, the EU will learn how to navigate the socio-technical and political-economic shifts that will proceed over the next couple of years, at rapid speed. Whereas even as little as 20 years ago, online platforms were simply considered emerging ‘markets’ or ‘technical conduits’ for market transactions – markets that had to be regulated – it has finally dawned upon most governments that platform ecosystems and the technical infrastructures upon which they are built have moved to the heart of society. And hence, the governance of platforms takes place at all societal levels: from the supranational to the national to the local and the institutional level. It requires the acute awareness of all legislative and political actors when it comes to policymaking; by the same token, professionals’ sensitivity to the implementation of public values in online environments – public as well as private – is indispensable to the creation of trusted policies.

‘Governing trust’ and ‘trust in governance’ are not a simple policy matter, but they are processes woven into the intricate cultural and social fabric of society. The governance of (European) platform societies cannot be considered distinct from technological systems, the companies that produce them and the users that deploy them. Neither can platform dynamics be viewed separately from the ways in which they interact with institutional systems – systems they govern and by which they are governed. And therefore, the two models of trust distinguished in this introduction – the institutional-professional versus the computational-corporate model – may not refer to a *shift* from the first to the second but may rather imply a *gradual amalgamation* of the two into a *distributed* model of trust. In fact, there is a lot at stake in the contest over what trust entails and how its governance gets distributed over the various actors in democracies. Rather than expanding existing formal systems for securing compliance and accountability, it may be more effective to foster cultures that support open societies and promote citizens’ capacities to judge trustworthiness, particularly in a society where digital automation is rapidly becoming the new normal.

Acknowledgements

I would like to express my sincere gratitude to the editors of the EJC and all six contributors for making this special issue possible.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This project which is part of the Policy, Expertise and Trust in Action

(PERITIA) project, has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 870883.

References

- Baghranian M (2019) *From Trust to Trustworthiness*. New York: Routledge.
- Bradford A (2020) *The Brussels Effect. How the European Union Rules the World*. New York: Oxford University Press.
- Braun JA and Eklund JL (2019) Fake news, real money: Ad tech platforms, profit-driven hoaxes, and the business of journalism. *Digital Journalism* 7: 1–21.
- Dolata UM and Schrape J-F (2018) *Collectivity and Power on the Internet. A Sociological Perspective*. Cham: Springer.
- Duffy B (2018) *The Perils of Perception*. New York: Atlantic Books.
- Dutton WH and Dubois E (2015) The Fifth Estate: A rising force of pluralistic accountability. In: Coleman S and Freelon D (eds) *Handbook of Digital Politics*. Cheltenham: Edward Elgar Publishing, pp. 51–66.
- Eavis P and Lohr S (2020) Big Tech's domination of business reaches new heights. *The New York Times*, 19 August. Available at: <https://www.nytimes.com/2020/08/19/technology/big-tech-business-domination.html>.
- Gillespie T (2010) The politics of platforms. *New Media & Society* 12(3): 347–364.
- Gillespie T (2018) *Custodians of the Internet*. New Haven, CT: Yale University Press.
- Gorwa R, Binns R and Katzenbach C (2020) Algorithmic content moderation: Technical and political challenges in the automation of platform governance. *Big Data & Society* 7: 1–15.
- Lewandowsky S, Smillie L, Garcia D, et al. (2020) *Technology and Democracy: Understanding the Influence of Online Technologies on Political Behaviour and Decision-Making*. Luxembourg: Publications Office of the European Union. Available at: <https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/technology-and-democracy>.
- Napoli P (2019) *Social Media and the Public Interest: Media Regulation in the Disinformation Age*. New York: Columbia University Press.
- O'Neill O (2020) Questioning trust. In: Simon J (ed.) *The Routledge Handbook of Trust Philosophy*. London: Routledge, pp. 17–27.
- Petit N (2016) Technology giants, the moligopoly hypothesis and holistic competition: A primer. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2856502.
- Plantin J-C, Lagoze C, Edwards PN, et al. (2018) Infrastructure studies meet platform studies in the age of Google and Facebook. *New Media & Society* 20(1): 293–310.
- Smyrnaiois N (2018) *Internet Oligopoly: The Corporate Takeover of Our Digital World*. Bingley: Emerald.
- Van Dijck J (2019) Governing digital societies: Private platforms, public values. *Computer Law & Security Review* 36: 105377.
- Van Dijck J (2020) Seeing the forest for the trees: Visualizing platformization and its governance. *New Media & Society*. Epub ahead of print 8 July. DOI: 10.1177/1461444820940293.
- Van Dijck J and Alinejad D (2020) Social Media and trust in scientific expertise: Debating the Covid-19 Pandemic in The Netherlands. *Social Media & Society*, DOI: 10.1177/2056305120981057
- Van Dijck J, Poell T and De Waal M (2018) *The Platform Society: Public Values in an Online World*. New York: Oxford University Press.
- Van Dijck J, Poell T and Nieborg D (2019) Reframing platform power. *Internet Policy Review* 8: 2. Available at: <https://policyreview.info/articles/analysis/reframing-platform-power>.