HARVARD Kennedy School
MOSSAVAR-RAHMANI CENTER
for Business and Government

Digital Realignment
Rebalancing Platform Economies from Corporation to Consumer

Dipayan Ghosh and Nick Couldry

October 2020

M-RCBG Associate Working Paper Series | No. 155

Mossavar-Rahmani Center for Business & Government
Weil Hall | Harvard Kennedy School | www.hks.harvard.edu/mrcbg

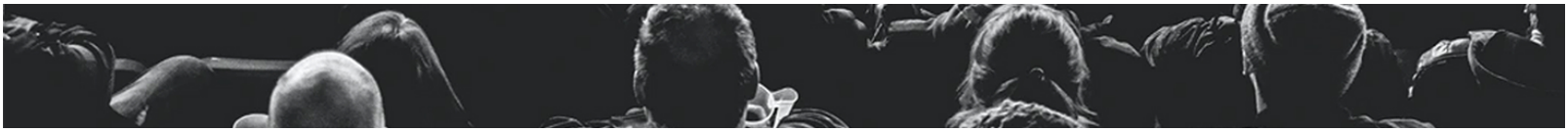
Digital Realignment

Rebalancing Platform Economies from Corporation to Consumer

October 26, 2020

Dipayan Ghosh

Nick Couldry



Digital Realignment

Rebalancing Platform Economies from Corporation to Consumer

Dipayan Ghosh and Nick Couldry

Harvard Kennedy School & London School of Economics and Political Science

October 26, 2020

EXECUTIVE SUMMARY

We are experiencing a fundamental evolution of the media ecosystem. Underlying today's global debate over the regulation of the online public sphere is a profound shift in the configuration of the social world: a transformation that grants to platform corporations a novel emergent power to shape the infrastructures, architectures, and spaces of social life. This transformation poses challenges not only for the regulators of markets but also for regulators concerned with protecting the good of society and democracy. That challenge has barely been defined or understood, let alone met.

Constant advancement of the technological base underlying global society is driving this massive change in the media. The challenges before us have emerged from technological developments, many of which were not initially conceived with such a profound social transformation in mind. However, the digital economy's trajectory – towards a public world profoundly engineered to favor commercial, not public, imperatives – was foreseeable long ago, even if then the dangers were at most speculative.

There is a new space of social interaction that is under commercial control. Three decades ago the internet began to develop on a commercial basis, as a privately sustained architecture based on myriad connections between computers. The space of social connection that emerged – "internet space," a creation of the consumer internet – has fundamentally different properties from pre-digital social space. The resulting consequences for society have depended on the rise of a business model that organically drives the commercial development and control of internet space.

A damaging alignment between corporate and bad-faith interests has taken root. For 15 years, two types of digital platform corporations – namely, information platforms such as Google and social media platforms such as Facebook – have implemented a business model that, with tremendous subtlety, has instituted a fundamental alignment in the persuasive interests of social actors and the commercial incentives of the platforms themselves. This has happened regardless of whether or not anti-social goals drive the former. Platforms manage the terms of that business model, which, to date, has not meaningfully been challenged by regulators. The result is a global commercialized infrastructure that facilitates the generation of social harms on a considerable scale and at extraordinary speed. Our digital infrastructure needs urgently to be **realigned**.

This Paper's Recommendations

We must renegotiate the balance of power between the corporate platform and the consumer. A new **digital realignment** is necessary. Achieving it will require decisive action that utilizes existing regulatory tools to their fullest capacities, but also designs new ones as part of a "regulatory reset" for today's consumer internet.

- *The priority of market reform*. The new contract involves, first, reform of the market behind digital media platforms – reform that would restore to consumers effective forms of privacy protection, thus enabling individuals to exercise real choice about how data that relates to or affects them is gathered, processed, and used. Such market reform would strike at one key way in which the business practices underlying the internet generate social harm, thus reducing their negative impact while also enabling markets to work better.

- *Mechanisms for combating social harms*. Market reform cannot be sufficient, at least in the medium term, to address the negative social externalities of the consumer internet. Needed also is the imposition of much greater transparency on platform corporations, uncovering not just their detailed operations but also the so far uncontrolled social harms from which they profit. The necessary response to those harms must confront them head on, requiring platforms to take urgent remedial action against controllable social harms, data collection that corrodes broader social values, and unregulated anonymity: those proposals, in turn, require adjustments to platforms' current blanket immunity from responsibility under Section 230 of the Communications Decency Act. If platform corporations fail to take such remedial action, as required by regulators, more drastic measures against the social harms associated with the consumer internet's business model, such as platform break-up, must be considered.

This paper provides a framework for the regulatory reset required to rescue a citizens' internet from the wreckage of today's consumer internet. Although, in some respects, legislative measures are more advanced in Europe than in North America, the report has relevance for both jurisdictions. With a U.S. presidential election approaching, the importance of these issues for the incoming administration could hardly be greater.

Table of Contents

Introduction

Society is not what it was. In this era of dominant digital platforms[1], we use the languages of social description and policy formulation inherited from earlier eras, but wonder why our existing regulatory tools fall short. The reason is so fundamental we can easily miss it: digital platforms have changed the very texture and dynamic of social life, requiring an urgent realignment of the resulting digital social world. Without this basic protection, contemporary societies will fail to address the forces that are making social and political life ever more toxic. This paper proposes the regulatory reset needed to confront the crisis in "platform societies".[2] Our proposals build on existing regulatory measures, particularly from Europe, but also go beyond them. The wider framework we advance has relevance both for North American and European contexts, and too can also help address forthcoming demands emerging from the Global South.

At the core of our approach is a commitment to taking seriously the consequences *for society* of what might otherwise be seen as exclusively economic matters: the operations of digital platforms. Humans have not lost the social and political limb of their existence, notwithstanding the challenges of the global pandemic. Indeed, that limb has been technologically enhanced: it is so easy to reach far-away people, hold four-way or 100-way video conversations, and so on. And we know this did not happen by magic, but via the commercial development of first, the internet and World Wide Web, second, digital platforms for commercial and social interaction, and third, the embedding of digital manifestations of all this in devices we carry everywhere we go.

Harder to grasp are the *consequences* of these commercial developments *for the texture of social life*. As a former Justice Department official has noted in reference to the Department's antitrust suit, "Google search is not a neutral gateway to the information available on the web," but rather "a set of algorithms designed to make Google — or

[1] Final Report, Stigler Committee on Digital Platforms, Stigler Center for Study of the Economy and the State, University of Chicago Booth School of Business, 2019.

[2] Jose van Dijck, Thomas Poell, and Martijn de Waal (2018), *The Platform Society*, Oxford University Press; Ron Deibert (2020), *Reset: Reclaiming the Internet for Civil* Society, House of Anansi Press.

Alphabet, its parent company — the most money it can possibly make." Nothing in history had prepared us for the idea that private corporations, motivated primarily by pursuit of profits, cannot just make products and services for social life, but literally redesign the spaces, and indeed the world, in which social life attempts to progress. Never until the past three decades have private interests been able to imagine, let alone achieve, such power over the basic design and intricate dynamics of complex societies. It is as if thirty years ago the world's societies had delegated to profit-seeking corporations the redesign and management of the spaces where human beings encounter each other, but without any discussion as to the possible social consequences.

Until now we have lacked effective tools to regulate this new form and forum of corporate power: we pretend it is just a continuation of older forms of economic and social power -- to compete in markets, organize economic production, or manage employees. Even the boldest recent proposals for reforming antitrust enforcement and law will likely fall short of meaningfully empowering consumers in the face of the commercial internet.[3] And while dominant internet platforms may indeed have taken some earnest steps to improve their corporate policy functions – as in the case of recent industry-wide commitments to act against content associated with the QAnon conspiracy movement in the United States[4] – these steps feel inadequate because they are partial, at the whim of platforms themselves, and fail to target the root of the problem. When, through market operations, large corporations – indeed, large and entrenched monopolies, as the recent U.S. House of Representatives Subcommittee report established – have acquired the power to *construct* social reality, this has implications for the quality of our social and political life, implications the require new regulatory solutions. Our goal in this paper is to outline a framework for formulating those solutions.

Until recently, much public debate about digital platforms has focused on the undesirable impacts of their automated algorithmic processes on information circulation or social discrimination. Very little debate has focused on the broader consequences for society that those platforms have, merely by existing on the scale they do and following the business model they do. Even the recent House antitrust report recognizes only the

[3] See e.g., Subcommittee on Antitrust, Commercial and Administrative Law of the U.S. House of Representatives Committee on the Judiciary, "Investigation of Competition in Digital Markets", 6 October 2020; "Top UK competition official threatens action against Google and Facebook," *Financial Times*, 18 October 2020; and France and Netherlands join forces to back EU move against tech giants, *Financial Times*, 15 October 2020. See also the antitrust actions under way in various jurisdictions against major platforms, most recently the action by the U.S. Department of Justice against Google, e.g. Rob Copeland and Tim Higgins, "Google's Exclusive Search Deals with Apple at Heart of U.S. Lawsuit", *Wall Street Journal,* 20 October 2020.

[4] Mike Isaac, "TikTok Cracks Down on QAnon and Hate Speech," *The New York Times*, 21 October 2020.

impact of platforms' anti-competitive advantages on 'economic and political liberties'.[5] All these are important, but fall short of the fundamental task for *societal* regulation today -- which is to recognize that private corporations, without exactly intending to, have over the past three decades acquired the power not just to provide services, but *to build new and unforeseen worlds* of persuasion, influence and control. In other words, multinational digital corporations have found themselves with novel *social* powers they barely understand, powers that, because they bring them relative advantage, they seek to defend and protect: social powers that, being corporations, they exercise for *commercial* purposes. The result is an impasse in how we regulate the digital world.

The problem can be condensed in a single phrase: the *"consumer internet"*.[6] This phrase is paradoxical: the internet, after all, is just a space of interconnection between texts, objects and people, and people certainly are much more than consumers. Why should interconnection by itself limit how we treat people? In principle it should not, yet the recent transformation of social and public life is based on such a reduction: the reduction of society's web of connections to relations of consumption which, in capitalist economies at least, corporations are implicitly given full license to manage. This is the result of the internet's increasing dominance by a small number of extremely large platforms and platform-like infrastructures[7] (notably Google, Amazon, Facebook, Apple), which not only provide key interfaces for the conduct of particular social interactions, but provide the basis on top of which much of economic, political and social life is now built.[8] Yet dominant internet companies regard platforms as *their* domain, disregarding the fact that those platforms have become the spaces across and through which *we* share our lives. Such corporations fail to grasp the full implications of their power, even as they exploit it. The "consumer internet" is what results when the vast open-ended space of online interaction and exchange becomes managed principally for profit. The result is *social* externalities that platform regulation has so far failed to confront – unsurprisingly, because the central framework for approaching platform regulation to date has been antitrust laws' concern with economic externalities.

The challenge for internet regulation in the 21st century is clear: how can governments, charged with regulating economies and societies for the public good, protect them from

---

[5] Subcommittee on Antitrust, Commercial and Administrative Law of the U.S. House of Representatives Committee on the Judiciary, "Investigation of Competition in Digital Markets," 6 October 2020, p. 19.

[6] Dipayan Ghosh (2019), "The Commercialization of Decision-Making: Towards a Regulatory Framework to Address Machine Bias over the Internet", *Hoover Institution papers,* spring series, issue 619.

[7] Jean-Christophe Plantin, Carl Lagoze, Paul Edwards, Christian Sandvig (2016), "Infrastructure Studies meet Platform Studies in the age of Google and Facebook'" *New Media & Society*, iss. 20, no. 1: 293-310.

[8] José van Dijck (2020), "Seeing the Forest for the Trees: Visualizing Platformization and its Governance", *New Media & Society*.

the excessive power represented by this corporatization of social life? Social life, after all, belongs to human beings, not corporations. As Milton Friedman argued,[9] businesses are not people; only people have the responsibilities that make up social life. This means that it should be people, not corporations, that take responsibility for how social life is managed, and it should be the values of people, not corporations, that underlie how we manage the impacts of platforms on social life. The challenge is to manage the digital economy with such social values in mind, as if indeed society mattered. We need a regulatory framework that can rescue a *citizens'* internet from the wreckage of today's consumer internet.

Our argument proceeds in two parts. In the paper's first half, we review the various ways in which society has been reorganized around platform power and the dangers this poses both for the fair operation of markets and wider economy *and* for the quality of social and political life. In the paper's second half, we present a framework, inevitably not granular, for combatting those challenges: first, strengthening significantly the privacy rights of consumers in their dealings with digital platforms and, second, proposing a range of measures designed to reduce the negative externalities that flow from the everyday operation of digital platforms' basic business model.

Why Platform Regulators Need Social Theory

The COVID-19 global health crisis has shown how the internet's networked infrastructure supports economic and social life. The internet allows new ways of conducting business when physical contact is impossible (online livestock auctions, restaurants shifting to online orders, food wholesalers dealing directly with consumers). The internet provides the means for basic socializing (WhatsApp, Zoom) and coordinated creativity (song parts recorded on phones or computers and mixed online). Much of today's broadcasting is sustained by broadcasters' operating from their homes, using their private internet connections! No one wants to return to the pre-1990s world of intermittent connection.

Some argue that our intensified reliance on online resources in the COVID-19 crisis counters recent criticisms of Big Tech,[10] or even that the "tech-lash" will be reversed.[11] But this is a non sequitur. Many of these benefits flow from internet connection, not from

[9] Milton Friedman "The Social Responsibility of Business is to Increase its Profits", *The New York Times,* 13 September 1970.

[10] Theodore Schleifer, "Google's former CEO hopes the Corona crisis makes people more 'grateful' for Big Tech", *Vox*, 14 April 2020.

[11] Editorial Staff, "Has the Coronavirus Killed the Techlash?," *WIRED*, 20 March 2020.

Big Tech platforms. Yes, we need to be connected in many of the ways we have become accustomed to over the past three decades, but not necessarily at the price of accepting the consumer internet. So let us survey the types of harm that have beset the online world in recent years.

Our discussion will focus on the digital platforms dominant in the West, but we acknowledge that platforms with comparable, maybe even greater, social power have emerged in China and elsewhere in the world. When considering remedies for those harms, our primary focus will be on the regulatory context of the United States of America, because it is there that the forces of the consumer internet are most weakly counter-balanced by public information institutions.[12] Because, however, the social costs of the consumer internet are global in reach, we will refer at times to European and other regulatory contexts. Our broader framework has relevance both for North American and European contexts.

Internet Space and some Familiar Online Harms

Much recent debate has focused on symptoms rather than causes, and used a moralizing tone which obscures structural issues. Take the furor over "fake news". Even leaving aside particular politicians' exploitation of this term for their own purposes, "fake news" discourse obscures more than it illuminates. There has always been misleading gossip and lies circulating at some level of society, while the problem of "churnalism" (false or misleading stories that circulate because journalists don't fact-check them sufficiently) was explained a decade ago by under-investment in news reporting.[13] The same applies to other features of online interaction which have induced moral concern: the rise of verbal and image-based abuse, mass murders inspired by a murderer's desire for notoriety. What is new are not abusive relationships or criminals' addiction to media attention, but the increasingly elaborate online architecture across which these human crimes play out.

Think about the space of connections made possible by linking computers online: what we'll call *"internet space"*. Its basic features are very different from previous forms of social space. First, *size*: internet space is infinite. There is no limit to the number of computers that can be connected to the internet, and connected computers can have

[12] For an important parallel argument grounded in the very different institutional setting of Europe, see Van Dijck et al. (2018), *Platform Society: Public Values in a Connective World*, Oxford University Press.

[13] Nick Davies (2008), *Flat Earth News,* Chatto and Windus.

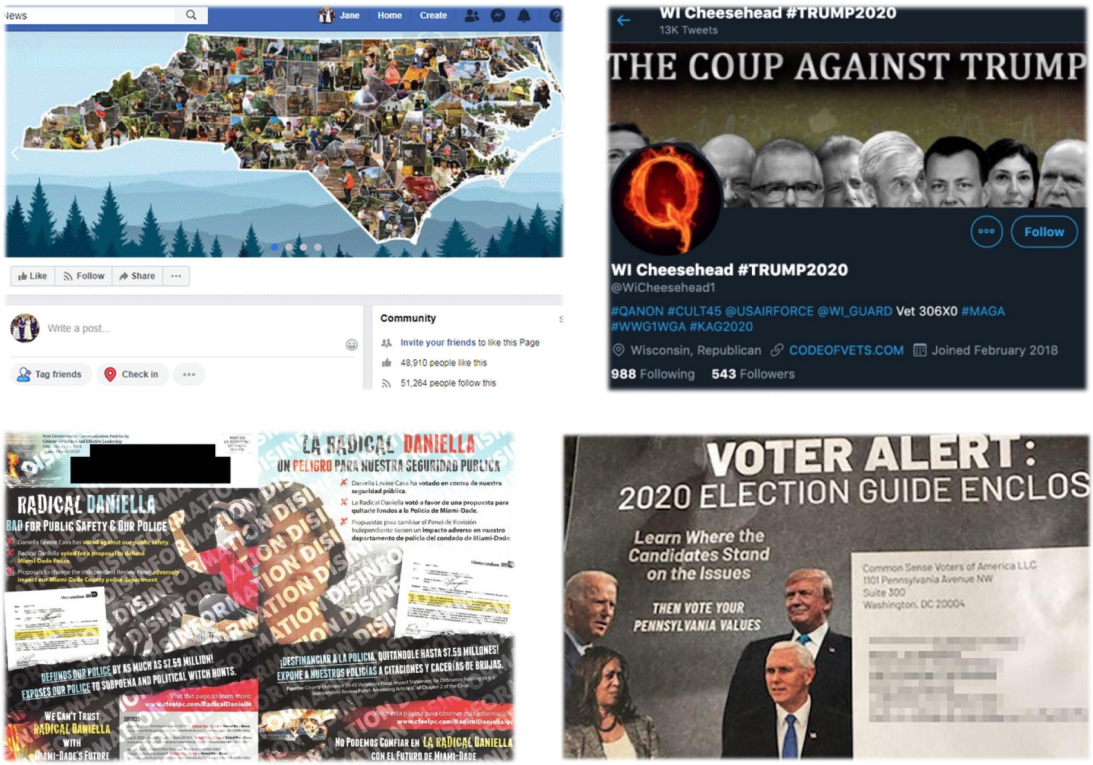


Figure 1. **Election disinformation is back in 2020**. The presidential and state-level elections in the United States have emerged as major targets for misinformation and disinformation, including, in clockwise order from top-left, in North Carolina[14], Wisconsin[15], Pennsylvania[16] and Florida.[17]

[14] Jane Wakefield, "North Carolina Facebook page labelled fake news," *BBC*, 18 February 2020.

[15] Max Witynski and Jessica Christoffer, "Skepticism Urged As Disinformation, Voter Suppression Wash Over Wisconsin," *Wisconsin Public Radio*, 16 August 2020.

[16] Em Steck, "Political group tied to Kanye West campaign law firm sent misinformation on Biden with mail-in ballot applications to battleground state voters," *CNN*, 4 September 2020.

[17] Nicholas Nehamas and Sarah Blaskey, "Disinformation, dark money, 'looting and rioting': 2020 election ads bombard Florida," The Miami Herald, 16 October 2020.

any relationship (real or fictitious) to people or organizations. “Bots” and “astroturf” are a residual feature of internet space, unlike offline space, which is limited by the number of human bodies in circulation. Second, *density*: limits on inputs to internet space are low, and the ability to upload inputs (photos, audio, video, text sources, text commentary) regularly, indeed continuously, is widely distributed. As a result, the “traffic” of internet space is many orders of magnitude denser than that of offline interaction. Third, *circulation scale*: inputs, once they enter internet space, can circulate over any distance at exceptional speed, limited only by the time that “viral” content takes to reach some part of each person’s internet stream. Negative effects of online circulation cannot be easily controlled, once circulation has started. Fourth, *incentives*: because internet space is infinite, density is high, and circulation hard to limit (the first three factors), the cost-benefits of doing harm online are very different from those that apply offline. In most offline contexts, there are real and immediate costs to insulting, abusing, and spreading rumor and lies: online, those costs are massively reduced.

These basic features of online space have alarming consequences. For example, they generalize the condition of pure rumor (with all its dangers for polluting human discourse) to social interaction as a whole, unless we build in structural safeguards against this. It matters therefore hugely how internet space is designed. Yes, with billions of voices online, almost all go unheard and ignored, so, without “media” of some sort to focus people’s online attention, almost all online voices would dissipate. But today not only traditional media but digital platforms (large and small) play a key role in focusing attention. The design choices of platform owners are therefore enormously consequential for the *type* of social space that emerges online.

Just one example: anonymity. A factor that prevents internet space from becoming just a rumor firestorm is verifiable identity. If someone spreading false or harmful information faces identification when they act, she risks being harmed in return at some point; anonymity by contrast is a way of avoiding those risks. The *social costs* of anonymity are generally controlled in offline society where, aside from situations of rumor, speaker identification remains a significant risk. But the structure of internet space, where people speak through computers and not their bodies, means that online the social costs of anonymity are many magnitudes higher than offline. Let’s imagine a platform where verifiable identity is not a requirement, where pseudonyms are allowed. On such platforms, the risks to speakers of lies or hate speech are massively reduced. In fact, allowing pseudonymous speech on platforms directly *incentivizes* harm through the resulting asymmetry between speaker and target. There are few greater disasters for a purveyor of online hate than to be “doxed”, that is, have his identity revealed and a

symmetry of harm restored.[18] Does this mean anonymity should be impossible online? That, as U.S. First Amendment scholar Danielle Citron argues,[19] is a step too far, because, online as offline, some people, particularly those who may unfairly face threats or harms from speaking identifiably, need anonymity in order to speak safely. But the problem remains, that anonymity incentivizes social harm. We offer a regulatory proposal at the end of this paper, but already this brief discussion illustrates that internet space poses novel problems for social order.

In what follows we offer some important background to this paper's approach and, in particular, the reasons why we foreground the social externalities of platform operations that other regulatory approaches, predominantly based on economic thinking, have neglected.

Social Design Matters

How internet space is designed is of social, not merely commercial, importance. The fact, noted by a number of analysts, that platforms are increasingly crucial to the organization of internet space (so called "platformization")[20] could be treated as a fact of nature, but it is smarter to see it as a form of social design. Until recently, we have thought of social design as the responsibility of society's members, with support from architects and other spatial designers. Over the past thirty years social design has become the responsibility of computer engineers, but unsupported by the evolving expertise about our spaces for physical interaction that has informed architecture over centuries.

Yet bad design of internet space – for example, platforms' original design to incentivize information circulation and data extraction over everything else - potentially creates major social externalities: a toxic *environment* for human interaction. Some have diagnosed a decline in the quality of information, a "corruption of the information ecosystem".[21] This could also affect the quality of human interaction, affecting interpersonal trust. Either way, the underpinnings of democratic culture are at stake and require monitoring by citizens or their representatives with an eye on the broader public

[18] For examples of "doxing", see Andrew Marantz (2019), *Anti*-Social, Viking.

[19] Danielle Citron (2014), *Hate Crimes in Cyberspace*. Harvard University Press, 221ff.

[20] Plantin et al. (2015) "Infrastructure Studies meet Platform Studies"; Anne Helmond (2016) "The Platformization of the Web: Making Web Data Platform Ready," *Social Media + Society* 1, no. 2.

[21] Karen Kornbluh and Ellen Goodman (2020), "Safeguarding Digital Democracy: Digital Innovation and Democracy Initiative Roadmap", *The German Marshall fund of the United States*, March, issue 4.

good.[22] Yet in the world of the "consumer internet", such decisions have been left almost entirely to corporations whose goal was never to design society, only to maximize profit.

This is all the more surprising when those engineering decisions deal directly with the operations of internet space, a space which, as earlier noted, is differently organized from physical space (being the result of myriad point-to-point connections). Engineering internet space is about much more than providing the containers (like rooms or buildings) in which human interaction goes on; engineering internet space affects the dynamics of all connections, transforming the texture and quality of our daily interactions. including their symmetry or asymmetry (for example, can someone on a platform reply to you or not?).

Historical models of social change have brought out the "civilizing" process that emerges through increasing social interaction and interdependence,[23] but this depends on the basic symmetry of most human interactions, which distributes the costs of anti-social behavior reasonably evenly. As we noted regarding anonymity, internet space may incentivize asymmetrical social interaction which is more likely to be "uncivilizing" than civilizing. As societies, we have barely begun to register the costs of encouraging asymmetrical models of online behavior. Yet such risks were foreseeable from the start, as we shall now see.

Computing's Forgotten Problem

There was always potentially a social problem with computing. The founder of the science of cybernetics, mathematician Norbert Wiener, realized this at the very start of the computer age. In the 1948 first edition of his classic book *Cybernetics* he wrote:

> "It has long been clear to me that the modern ultra-rapid computing machine was in principle an ideal central nervous system to an apparatus for automatic control . . . Long before Nagasaki and the public awareness of the atomic bomb, it had occurred to me that we were here in the presence of another social potentiality of unheard-of importance for good and for evil".[24]

[22] Julie Posetti and Kalina Bontcheva (2020), "Challenges and Recommended Actions, Balancing Act: Countering Digital Disinformation While Respecting Freedom of Expression," International Telecommunications Union.

[23] Norbert Elias (1994), *The Civilizing Process*, Blackwell.

[24] Norbert Wiener (1961) *Cybernetics, or, Control and Communication in the Animal and Machine.* Martino Publishing, 27.

Wiener's point was probably not that computers are a channel for pre-existing human evil, or a political conspiracy to rule the world through computers. His point was probably subtler: that the structure of universal connection across space that computers enabled (the 'social potentiality' of computer-based connection) *itself* brought new possibilities of control, and so new forms of social force. Wiener's insights have recently been recalled in debates on the future of artificial intelligence.[25] But six decades after Wiener published his prognosis, it has had surprisingly little influence over society's use of computers.

The consumer internet's developers ignored Wiener's fears entirely, and prioritized corporate interests that saw designing platforms for social life as just an engineering problem, at most a matter for management or organizational theory, "solvable" without regard to the sorts of computer-enabled social externality that Wiener had feared. The problem was so simple that it was easily overlooked: where the engineering task is to design the control interfaces for social life, and where what is built becomes a default location for social interaction, then wide-ranging social externalities may result from those interfaces' design features, which, if both negative and stable, generate environmental harms. When platforms, through our intense use of them, become not just individual services, but connected *ecologies* for everyday living,[26] then the significance of the engineering decisions that underlie those platforms is rescaled. What once were imagined as merely engineering decisions suddenly morph into designs for the ecology of social life. Social life itself becomes reengineered.

The ecological problem of today's computer-based platforms arose from three cumulative developments, none of them malevolent. *First,* computers, as part of their basic functioning, track themselves: they build an archive of the various changes of state through which they pass, an archive which forms the basis for each computer's capacity to function. This tracking capacity of computers is not itself surveillance, but it is the seed of computers' wider powers of social surveillance.[27] *Second*, through the commercialization of the internet in the mid-1990s, computing devices became by default connectible with other computing devices via the internet, with the Internet of Things being only the most recent extension of this phenomenon. As a result, computers became capable not just of tracking themselves, but of tracking each other. As information scientist Philip Agre noted more than a quarter-century ago,[28] the surveillance implications of connected computers depend entirely on the social uses to

[25] Stuart Russell (2019) *Human Compatible.* Allen Lane, 136-138.

[26] Nick Couldry (2019) *Media: Why It Matters.* Polity, chapter 1.

[27] Philip Agre (1994) "Surveillance and Capture: Two Models of Privacy." *The Information Society* 10, no. 2: 101-127

[28] Agre, ibid.

which computers are put. The first two steps would not by themselves have had major consequences without a *third* step: the exponential growth of computer processing power and memory since the early 1990s to store the outputs of continuous computer-to-computer surveillance. The result of the three steps taken together was the emergence in societies of all sorts, democratic and authoritarian, of a powerful networked instrument with the potential for social surveillance, influence and control.

It is possible that, if the internet had remained under public control, its development path would have been different. But, through a US political decision made in the early 1990s,[29] the internet transitioned from a state-owned network to a commercially operated system. From then on, the internet was free to become a vehicle for the pursuit of corporate power and its advertising and marketing interests, but always with the possible implications for social power and democratic life that, as we just noted, were built into the rollout of computers in society from the start.[30]

Everything depended on the model then chosen for the internet's further development. What was chosen was the model we have called the consumer internet. Prima facie just a business choice, this path generated social externalities, as Norbert Wiener anticipated. Those externalities are too severe to be ignored if we care about the quality of contemporary life.

Let us look in more detail at the business model of the consumer internet, remembering that, for reasons just explained, this model was always also, even if unwittingly, a model for redesigning *society.*

The Consumer Internet, or the Corporate Harvesting of Social Knowledge

The laissez-faire tradition of governmental industry oversight in the United States of America has allowed the typical consumer's relative economic power vis-à-vis the digital platform sector to reach a strange state: s/he has none. This is one fundamental reason why as consumers and citizens we find it difficult to address the consequences of platform operations for society.

---

[29] The U.S. government's decision to close NSFNET which had run the internet's underlying structure and transfer that role to commercial internet service providers was described by John Doerr, partner at venture capitalists Kleiner Perkins Caulfield & Byers as "the largest creation of legal wealth in the history of the planet": cited, Andrew Keen (2015) *The Internet is Not the Answer,* Atlantic Books, 38.

[30] Paul Schwartz (1999) "Internet Privacy and the State." *Connecticut Law Review* 32: 815-859; Ethan Zuckerman, "The Internet's Original Sin," *The Atlantic,* 14 August 2014.

As the world witnessed the revolutionary expanse of the big data economy – with tremendous increases in computing power and data storage combining to enable corporations to collect inordinate amounts of data – the digital media sector quietly built a novel commercial regime premised on such data collection. Regrettably, the resulting asymmetry of power between consumer and corporation has fueled monopoly power in the new media landscape,[31] and removed consumer choice with dangerous consequences for democratic societies globally.[32] Governments everywhere must now place power back in the hands of the consumer - the consumer who is also, of course, a citizen and a member of society. But how?

One way forward is to restore the basic features of privacy that it has been normal to protect in capitalistic markets. By privacy we mean, the affordance to the consumer of the power to know what is being collected on her, comprehend the meaning of that collection for her and her community's democratic interests, and intelligently make the personal data-governance decisions she deems right.

Another is to reform privacy and platform functioning in the context of a radical reset of the regulatory framework for thinking about the corporate products (platforms) on which so much of daily social life is conducted today. Our immediate regulatory focus in what follows will be the United States of America, but debate is needed in many countries about how online privacy can seriously be defended and how sufficiently robust regulatory frameworks can be built.

This will be no easy feat. The market not only has generated monopolies throughout every subsector of the consumer internet, including social media, email, online search, internet-based text messaging, online video sharing, and e-commerce, but done so in ways that affect the very fabric of social life. It cannot be sufficient just to let capitalistic markets take their course, as U.S. regulators have generally and traditionally preferred.

The U.S. government must now consider mechanisms by which it can rebalance the severe asymmetry of knowledge and consumer power via privacy regulation in the democratic and market interest. If it fails to act, then regulatory authorities in competing nations may develop stronger digital governance norms at the expense of American economic interests. There are already clear signs that European regulators are planning

---

[31] Or, more complexly, monopoly/monopsony power: Nick Couldry and Ulises Mejias (2019) *The Costs of Connection*. Stanford University Press, chapter 2.

[32] The Australian Competition and Consumer Commission summarizes the asymmetry of power in the consumer internet industry, noting in that these firms "leverage digital platforms' bargaining power and deepen information asymmetries, preventing consumers from providing meaningful consents to digital platforms' collection, use and disclosure of their user data." (See: Australian Competition & Consumer Commission, "Digital Platforms Inquiry," 26 July 2019.)

bold moves that may include calling for the break-up of dominant internet companies:[33] if implemented, other countries may follow suit, as happened in the wake of the EU's 2018 General Data Protection Regulations, on which more soon.

First, let us look closely at the economic core of the problem.

How Personal Data is turned into a Corporate Asset

That core is the consumer internet's distinctive business model. The corporate commoditization of personal data did not take place overnight. Only as certain executives at the digital platform firms came to understand their vaunted position in the market and the effect the big data revolution could have on their industry, did a new business model take shape.[34] That business model has come to favor a three-pronged model for monetizing platform users: first, the *collection* of data on the user so as to generate behavioral profiles; second, the refinement of sophisticated *algorithms* that curate the content in her social feeds and target ads; and third the sustaining of engaging – and perhaps addictive – *content* on platforms that keep her hooked, to the exclusion of rivals. If we are to challenge the practices underlying this cycle – and, in particular, the collection of data on the user – we need to reset the regulatory framework.

The transformations needed must start from the data operations at the business model's core. Through their years of operation, dominant digital platforms such as Google and Facebook have developed robust mechanisms by which to collect and process raw data on the individual user, and convert that data into behavioral inferences that contribute directly to their economic model. It is not within the scope of this paper to fully outline the myriad pathways through which platform monopolies acquire such data.[35] The one-sided relationship of data transfer from the user to the platform begins on day one. Immediately after the user signs up for the service, her personally identifiable information, perhaps including her name, phone number, and email, are collected. The corporation thereafter typically generates a log-on ID to associate with the individual – such as a Twitter handle, Gmail address, or Facebook UID. With the relationship

[33] Javier Espinosa, "EU Targets Big Tech with 'hit list' facing tougher rules", *Financial Times,* 11 October 2020; Javier Espinosa and Mehreen Khan, "France and Netherlands join forces to back EU move on tech giants", *Financial Times,* 15 October 2020; Kate Beioley and Javier Espinosa "Top UK competition official threatens action versus Google and Facebook", *Financial Times,* 19 October 2020.

[34] Our focus will be on this business model and its consequences. We leave aside the question of how we characterize the wider transformation involved but see, e.g., Shoshana Zuboff (2019) *The Age of Surveillance Capitalism.* Profile Books; Couldry and Mejias (2019) *The Costs of Connection.*

[35] Dipayan Ghosh (2020) *Terms of Disservice.* Brookings Institute Press.

established, the platform will typically begin collecting large amounts of on-platform engagement data associated with the individual – information concerning, for instance, which social media posts the user hovered over, which media personalities and musical artists and politicians she chooses to follow, which third-party web URLs she clicked on, how long she spent on those third-party websites and what their content was, and so on. Quietly, the platform will typically also begin to acquire "off-platform" data on the user, which might emerge from direct relationships with the platform corporation (e.g., agreements to share fine-grained location data tracked by smartphones with its mobile applications) or indirect relationships the platform corporation establishes with unknown third parties such as data brokers or other recognizable brand name companies. This third-party data might detail the individual's financial transactions, precise geolocation, biometric information (e.g. facial recognition metrics), web browsing history, social graph, and mobile ecosystem usage data among other possible sources. And over time, the corporation might determine that this particular user represents a high-value customer given her spending capacity, and choose to acquire even more data on her personhood from those sources and more.

The platform corporation's intent is clear: to generate a behavioral profile that explicitly predicts the likes, dislikes, interests, preferences, beliefs and routines of the individual user. This information – which powers the ranking of the user's social feeds and determines the channeling of ads targeted at her – is the central unifying function of the platform corporation's economic logic and defines the algorithmically-automated pathways of content curation, ad-targeting, and media manipulation to which the user is systematically subjected over time. On its basis, other services – indeed a whole infrastructure for social and economic life – has been built.

These business developments have profound impacts for how markets today function.

The Distortion of Economic Space

The result is to distort not just social space (as suggested earlier in the paper), but also economic and market space. Let's look at some ways in which the outcome diverges sharply from standard market situations.

The first feature is that the consumer *hugely discounts the value of her personal data*. Discounting of some sort is a feature of many market situations: when given the option of accepting currency now or the same time-adjusted amount of currency in the future,

people typically choose the former.[36] This irrationality applies to an intense degree in the privacy bargains that platform consumers make. Users often fail to consider the full effect of data collection and monetization by firms – precisely because they fail to recognize the *future* value to them of keeping that information private (and the future harms – economic, social, psychological – that may result from failing to do so). When the typical customer signs up for a social media service, she does not usually consider that subscribing now might implicate the privacy of her data when exposed to a cybersecurity breach five years later – or perhaps even worse, when her vote is manipulated by Russian disinformation operators fifteen years later. This mass devaluation of privacy by consumers – whether "naïve" or "sophisticated," to use the language of behavioral economist Acquisti – has long been exploited by platform corporations and now constitutes a major economic/social asymmetry of platform space.[37]

The second distortion is the "price-inelastic" nature of the relationship between consumer and platform corporation. Assuming that the consumer's data and attention equate to economic value *for the corporation*,[38] consumers engage in relations of data transfer with the corporation which are highly price-inelastic. In effect, the consumer participates on the firm's platform without regard to the actual value set on her data behind the scenes, which is *highly variable*, as measured in the complex way the consumer internet industry understands, that is, in terms of combined consumer data and attention. And yet the value the consumer gets in return remains *exactly the same*: use of the platform. When we sign up as consumers for the platform service, simply by accepting its terms of service and privacy policy, we enable *unlimited* data transfer from consumer to corporation, but in return for a fixed benefit. It is not clear what consumers think of this unbalanced transaction (they may be resigned to it),[39] but acceptance of such price rigidity must, in part, be driven by their perception of the essentiality of the service in question, and the lack of alternatives. But this is not how any economic relationship should be structured; it should favor fair economic exchanges based on mutual understandings of the actual value at hand.

---

[36] Richard Thaler (1981), Some Empirical Evidence on Dynamic Inconsistency, *Economics Letters*, (3): 201–207.

[37] Alessandro Acquisti (2004), Privacy in electronic commerce and the economics of immediate gratification, *Proceedings of the 5th ACM Conference on Electronic Commerce*, New York.

[38] We are not assuming that such data *should* be commodified, and later ask whether certain data should be collected *at all*.

[39] Joseph Turow, Michael Hennessy, and Nora Draper (2015) "The Tradeoff Fallacy: How Marketers and Misrepresenting American Consumers and Opening Them Up to Exploitation", Annenberg School for Communication, University of Pennsylvania.

The Economic Effects of Harvesting Personal Information

In activating this economic logic, digital platforms have ushered in an insidious new economic reality: rank exploitation of individual consumers' private information. Currently there is no regulation in the United States that prevents this. As such, given their control of the market, large digital platforms do not hesitate to take advantage of the harmful impacts on consumer psychology.

There is a vast physical-digital infrastructure underlying platforms' capacity to pursue such exploitation. This infrastructure entails the vertical integration of all capacities from bottom to top of the technology stack: massive server farms and commercial arrangements with telecommunications firms that enable seamless consumption of their platforms, inordinate amounts of data collection that unlock exclusive knowledge of users and the industry, and sophisticated artificial intelligence systems that hone content recommendation and ad targeting systems to such a degree that users are unable to find a 'better' experience elsewhere. These hallmarks of the digital platforms allow them to monopolize the targeting-and-tracking regime on which today's media ecosystem has come to depend. And they generate the negative social externalities – from the spread of hate to the disinformation problem – that we witness today.

An economic consequence of platforms' vertical integration is market bottlenecks. Platform corporations exclusively have the most complete and compelling knowledge about the individual. They exclusively possess and operate the platforms over which those users engage and interact, benefiting exclusively from the resulting network effects; and they exclusively possess the physical infrastructures necessary to operate such universal platforms. The result is diminished capacity for new innovation. Any fledgling that attempts to supplant the platform monopolies' positions must either fail because it cannot compete with the infrastructure underlying the economic incumbents, or join the Goliath by being acquired.

The consumer internet is today composed of one market monopoly after the next: social media, email, internet-based text messaging, search, e-commerce, online book sales, online video – each of these is dominated in most democratic economies by one firm, by one business owned by Amazon, Facebook or Google. In market democracies, monopolies are not wrong. But a monopoly position may not be acquired or maintained illicitly, or wielded so as to suppress the innovations of would-be competitors.

But that is precisely what is happening now. Facebook, to take one example, has monopolized the social media space; it is the dominant firm in consumer marketplaces

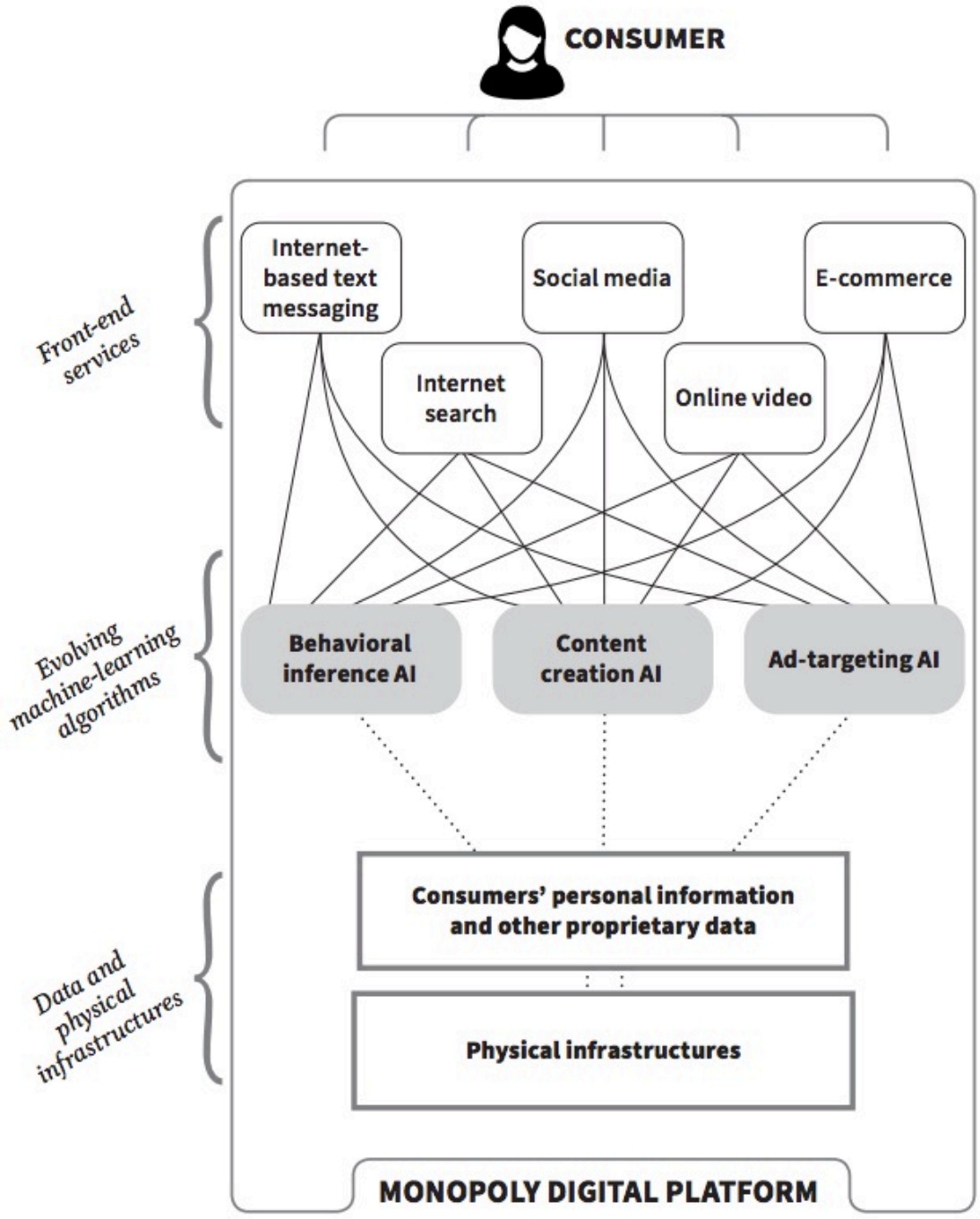


Figure 2. **A damaging business model**. Dominant digital platforms maintain powerful digital and physical infrastructures through which they rake consumer data and attention at monopolistic rates, use behavioral information to maximally keep users engaged to curated social content, and target personalized advertising to capture profits at margins exploitative to the rest of society and disruptive to the democratic discourse.

like the United States. With this dominant position, lent by its namesake and the Instagram and WhatsApp apps, Facebook can extract monopoly rents from its customers. It is often argued in the industry that there is much competition to receive digital advertising dollars – Facebook competing with the likes of Google, Amazon, and many other smaller platforms and digital media networks. But it is not in this particular market that Facebook has its monopoly. Facebook – and other consumer internet platforms – are two – or multi-sided markets that also engage directly with end consumers. It is in the latter market where they have their monopoly position, that enables the extraction of monopoly rents from our data and attention. Other large players benefit from parallel monopolies in online search, online retail, and devices.[40]

Such monopolies lie at the heart of the consumer internet and its consequences not just for economic but also social and political life. At stake therefore in addressing market distortions is much more than economic regulation: the wider social implications that flow from those market distortions require a wider regulatory framework.

The Consequences for Democracy

Recent times have illustrated that digital platforms enable a vast array of negative externalities – threat of disinformation, spread of hate speech, encouragement of algorithmic bias, and incitement to violence among them. These toxic outcomes might seem like a matter of mere cultural change, but we can draw a direct line from the data-driven economic model of digital platforms to the practice of uninhibited data collection and the corresponding profiling of the individual.

Take for instance, the disinformation problem. Assume, as seems reasonable, the intent of Russian disinformation agents is to subvert the functioning of American democracy; this facilitates the political ambitions of President Vladimir Putin. One potential method of projecting political lies and conspiracy with cost efficiency is to identify the thin cracks in the fabric of American society, the communities for whom such content will most effectively resonate – a few thousand American voters in Wisconsin, Minnesota, and Pennsylvania for example – and shower them with disinformation until those thin cracks fissure.

What is the connection with the business model of the consumer internet? It derives from the global reach of the information-gathering enterprise of the digital platforms; the

[40] Subcommittee on Antitrust, Commercial and Administrative Law of the U.S. House of Representatives Committee on the Judiciary, "Investigation of Competition in Digital Markets", 6 October 2020.

capacity to micro-target digital advertisements and intelligently channel organic content in such a manner that political conspiracy will project throughout an election season. This model is what enables a disinformation operator to access targeted communities – communities defined by their personal data and the behavioral inferences platforms and others have drawn from it. The consequences of hate speech, incitement to violence, and algorithmic bias are driven by similar effects concerning our personal data; we suffer these because of the exploitative collection of personal data, without which the platform algorithms that curate social content, profile people, and target ads at us would become far less effective.

It might seem surprising to connect such political consequences to the operations of a business model. But, if we accept the premise of this paper's first section -- that, when platforms become default social interfaces, their engineering choices directly impact on the ecology of social life (which includes political interactions too) – the consequences flow simply from the continued operation of the incentives built into the business model itself.

Platform Owners' Responsibilities and the Responsibility of Regulators

Let's bring together the various economic and social harms that we have examined so far in this paper. What do they amount to? Put simply, they amount to the direct management of key domains of social life so as to maximize profit – *whatever the cost to social, political and market functioning*. The consumer internet thus becomes a machine for producing negative social externalities on a huge scale, matching the unlimited scale on which internet space itself now operates. Only a complete regulatory reset can remove these multiple negative externalities platforms generate and better realign our digital world in accordance with social goals.

There is nothing wrong in businesses managing their production stream: that is a basic principle of market societies. But, as explained, a distinctive feature of contemporary societies is that their interfaces and platforms do double work: not just as production streams, but also as places where *social interaction* goes on, *social knowledge* is generated, and *publicly relevant information* is circulated between people. Who on behalf of society monitors the consequences of this double work? Platform developers and owners cannot represent "society". They are businesses pursuing their own profit, first and foremost. Society needs to develop an alternative site for monitoring how platforms affect our shared social life. Historically such monitoring responsibilities have been vested in regulators. But today's challenges require a broader conception of their regulatory responsibilities.

Regulators had never before expected to monitor how corporations design society, for the simple reason that corporations had not until recently expected to be in the business of designing society. Now, for the reasons unpacked at the start of the paper, they are. So a novel question arises: *What does it mean to design responsibly (i) the spaces where human beings interact, (ii) the social interfaces across which they transact, and (iii) the mediums through which private individuals (as opposed to powerful institutions) within and across national borders circulate information and express opinions?* Media law (e.g. law on free speech, defamation) will be of only partial help here, because it only deals with local harms. The challenge we face however is environmental: the emergence of general harms that flow from digital platforms' new role in engineering society. The resulting harms can truly be called toxic: that is, higher-order harms to the social environment caused by the malfunctioning of platforms or any other part of internet space and its infrastructure.

The notion of toxicity already raises questions of corporate responsibility, but digital platforms, as environments for social interaction, raise more complex questions than simply 'polluter pays'. For sure, some participants on digital platforms directly introduce toxic materials and so may be pursued under existing law. But regulators also need to think about the consequences of platform *design* (and the business model that drives such design) for the quality of interactions on a platform. As legal theorist Julie Cohen notes, 'platforms supply infrastructures that facilitate particular types of interactions', making particular 'clusters of transactions and relationships stickier' via a system of 'protocol-based control'.[41] Another legal theorist, Karen Yeung, calls this power vested in today's social designers (the platform owners) the "hypernudge":[42] the ability by channeling interaction in a bounded environment (such as a proprietary platform) to shape people's choices, indeed their *choices about* choices. Why would society want to delegate such a "behaviorist" power to *any* institution,[43] let alone institutions concerned exclusively with the pursuit of profit, rather than social good?

[41] Julie Cohen (2019) *Between Truth and Power*. Oxford University Press, 41-42.

[42] Karen Yeung (2017) "'Hypernudge': Big Data as a Mode of Regulation by Design." *Information Communication and Society* 20, no. 1: 118–36.

[43] On today's new "behaviorism", see Antoinette Rouvroy (2012) "The End(s) of Critique: Data Behaviourism versus Due Process." In *Privacy, Due Process and the Computational Turn*, eds. Mireille Hildebrandt and Ekaterina de Vries, 143–67. Routledge.

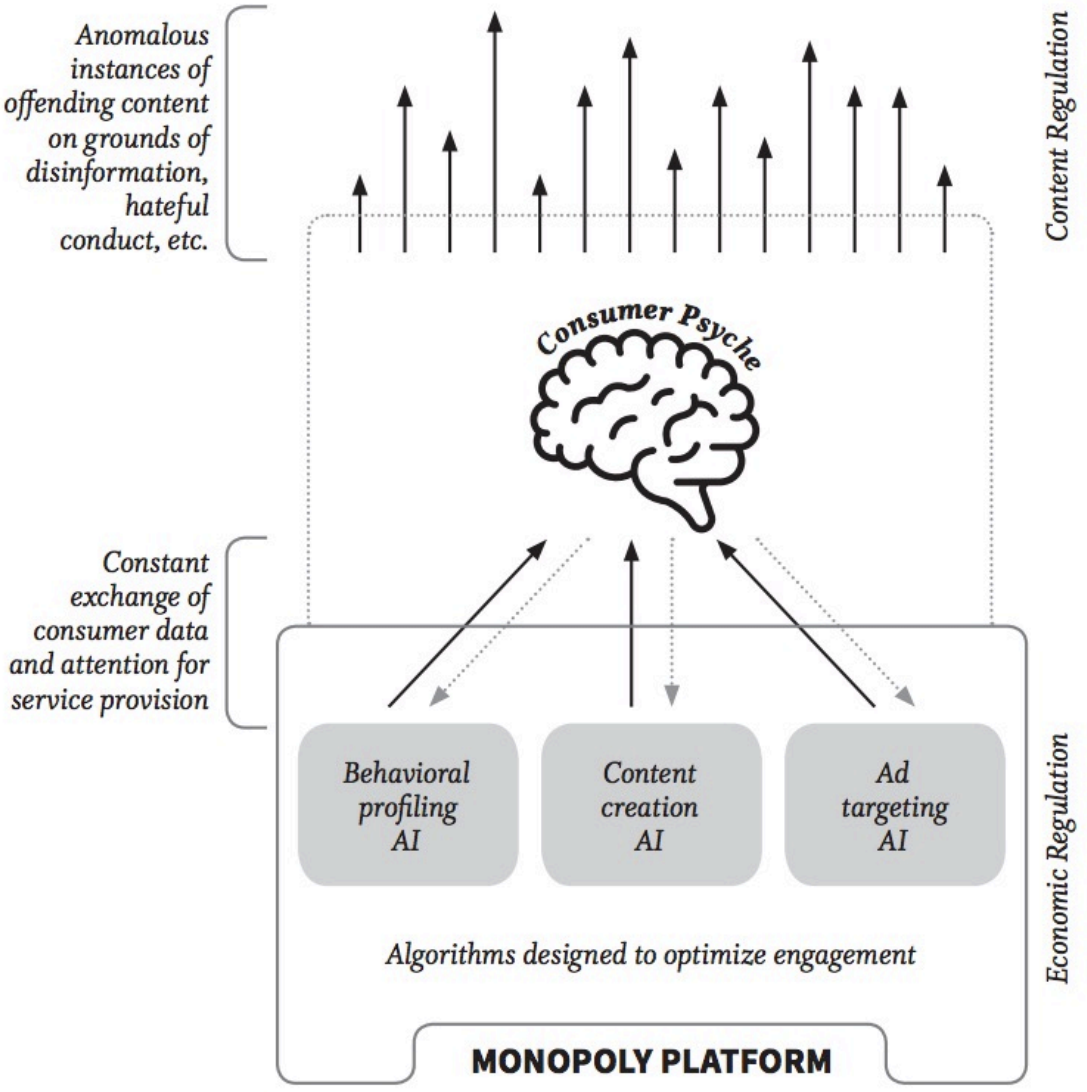


Figure 3. **The logic of internet-based content negative externalities**. The central problem behind the many negative externalities prevalent over the internet – the disinformation problem, the spread of hate speech, the impact of online violence, algorithmic discrimination, and myriad others – is the business model of the consumer internet itself. This has promoted an economic logic that aligns the commercial imperatives of internet platforms and persuasion interests of marketers – including bad actors.

Yet, once we acknowledge the remarkable new powers of social design that have been ceded to corporate platform owners in the digital age, we must also acknowledge their ability to *design out* such structures. Platform owners can and must take legal responsibility for the social consequences of their designs taking effect in the social world. The only reason for absolving platform owners from legal responsibility would be if we believed that private economic benefits automatically override social, indeed ecological, costs. But there is no ecology for living where we hold such a counter-intuitive belief.[44]

What therefore would it mean to *reset* the Internet's regulatory framework on the basis of taking seriously platform owners' responsibilities not just for their business models – they are, to a degree, responsible for them to their shareholders – but also for those models' negative social consequences?

A New Vision for Internet Regulation: Toward a Digital Social Contract

At the center of all the problems concerning the modern consumer internet is a subtle bind that has deeply incised contemporary societies and their potential for democracy: whatever platforms' pro-social claims, *the commercial incentives of the dominant digital platforms and the political and social imperatives of bad online actors are in deep and largely hidden alignment.* To the extent that consumer internet platforms will prioritize maximal consumer engagement at the expense of all else and enable a content-targeting infrastructure that acknowledges social consequences only as an afterthought, disinformation operators, hate speech propagators, and other nefarious entities will have multiple opportunities to push their toxic content. The risk of bad actors is not excludable: there will always be bad actors who wish to cause division in democratic societies, and today's explosion in availability and effectiveness of digital tools and expertise makes them ever more salient. The onus, then, must fall on the platforms that dominate and profit from the consumer internet to take steps to better meet society's and democracy's interests, failing which we must look to legislators and the regulatory community to enforce the necessary course corrections.

The costs of disinformation, hate speech, terrorist engagement, incitement to violence, algorithmic bias, various forms of economic, political and social exploitation: these are seemingly daily occurrences on the dominant digital platforms of the day. It is becoming

[44] As Julie Cohen notes, the "public domain" of platforms "subordinates considerations of human well-being and human self-determination to the priorities and values of powerful economic actors" (*Between Truth and Power*, 73). Market regulation is supposed to correct such inappropriate wielding of economic force.

increasingly apparent that digital platforms are not well-positioned to do anything about these serious problems. They face a direct conflict of interest: suppress these negative externalities, and thereby necessarily offend bad actors and their powerful allies, or just do nothing? Consider the speech given at Georgetown University by Mark Zuckerberg in late 2019 in which he touted his adherence to free-speech norms.[45] It is a convenient position that at once assures he does not invite Donald Trump's regulatory ire, does not set off a global intellectual discussion about where the red lines defining what is good and bad content should be drawn, allows particularly engaging (albeit divisive) content to stay online and drive further engagement, and does nothing to upset the President's political base – which, as reports suggest, uses Facebook in huge numbers.[46] Indeed, reports suggest that Zuckerberg – along potentially with chief executives of other large technology firms in California – has worked to assuage the fears of conservative U.S. politicians that social media firms will take down far-right speech in exchange for a favourable stance on the company's efforts to secure its dominant market position in the United States and around the rest of the world.[47,48] Facebook and other firms in the sector may in fact need to show more robust action, even if it means acting against the president's posts; research has shown that the most substantial source of misinformation is the president's Twitter account.[49]

Zuckerberg's recent speech is however merely the symptom of the longer-term problem we must confront: that *dominant digital monopolies are unilaterally and increasingly influencing the course of our democracy.* That may not necessarily be a harmful circumstance – provided that adequate and appropriate restraints are applied to those monopolies. Today they are not. Much regulatory work around the world – in parts of the United States, the UK, France and Germany, but critically also Argentina, India, Japan and Malaysia – is underway to correct the situation. Much of it is headed in the right direction, but until now we have lacked an overall practical framework that connects the industry's uninhibited data collection and opaque algorithmic manipulation of the consumer's digital media experience with a set of clearly defined harms, against which regulatory action can be recommended.

---

[45] Tony Romm, "Zuckerberg: Standing For Voice and Free Expression," The Washington Post, 17 October, 2019.

[46] Kevin Roose, "What if Facebook Is the Real 'Silent Majority'?," *The New York Times*, 27 August 2020.

[47] Georgia Wells et. al., "Facebook CEO Mark Zuckerberg Stoked Washington's Fears About TikTok," *Wall Street Journal*, 23 August 2020.

[48] "TikTok sale saga may play into Facebook's hands," *Financial Times*, 20 August 2020.

[49] Sheryl Gay Stolberg and Noah Weiland (2020) "Study finds 'single Largest Driver of Misinformation': Trump", *New York Times,* 1 October, citing Sarah Evanega et. al. (2020), Coronavirus misinformation: quantifying sources and themes in the COVID-19 'infodemic,' Cornell University.

We thus offer a framework for regulatory reform of the consumer internet in two parts: first, focusing on the fair functioning of the consumer internet market; and second, managing the broader social harms that have arisen from the consumer internet's business model. Under the first slate of our proposed regulatory regime, consumers are empowered to manage their personal situation through a reformed consumer internet marketplace, that better protects privacy, better promotes market competition, and better establishes adequate transparency over business. In the second, it is the government that must act to bar the industry from engaging in certain practices, which harm the social and democratic interest. Our framework, while not granular, is offered as an outline of the *range* of interventions now required. Taken together, this approach addresses both the social *and* economic negative externalities of the consumer internet's problematic business model.

Towards Better Market Functioning

Appropriate policy interventions are needed, first, to promote individual privacy rights, introduce algorithmic transparency, and enhance genuine market competition in the digital media sector to the end of transferring economic power from platform to consumer.

A New Approach to Privacy: The Redistribution of Economic Power

The typical user of consumer internet platforms – the fisherman in Chittagong, merchant in Tanzania, college student in Mexico City, teenager in London – pays little to no attention to her personal digital privacy, because she has more immediately pressing matters on which to focus. She freely gives her personal data to platform firms like Instagram and YouTube, whether on-platform or through off-platform browsing and engagement that leads to data being transferred back to platform corporations such as Facebook and Google. This is true even in cases of privacy-sensitive individuals; in the absence of other networks of connection that don't depend on the consumer internet, the imperative of being *on* the platform that all of one's friends and colleagues are using frequently overrides any personal consideration for privacy *for all users*. As she succumbs to that imperative, a threshold is crossed: now, so long as she is logged into these services, they can collect information on her without her awareness or understanding of the underlying implications. Further, she has no recourse to act as the member of a bloc or union of sorts of users; there is limited coordination among users given various circumstances special to the case of the consumer internet platform, including its global nature.

There is enormous scope for a fundamental privacy regulation to benefit consumers everywhere, giving the individual much greater say over what data can be collected and wielded by commercial providers. A very promising starting-point here has been made in a major jurisdiction: the European General Data Protection Regulation. The law, which came into effect in 2018 and involved multiple prior years of development, establishes a theoretical basis for exactly the sort of redistribution of power from corporation to consumer proposed here, that is, via serious attention to individual consumer rights. The granting of consumer access to information about how the corporation engages in collecting and processing data; the right to access one's personal data held by the corporation in question and to withdraw previously given consent for the processing of one's data; the right to be forgotten; the right to object to automated processing; data portability; and more – these are important mechanisms that *potentially* place substantial power back in the hands of the consumer. Concerns certainly exist about whether even this major legislative intervention is sufficient to change the relationship of force which, as we noted earlier, distorts the very possibility of valid consumer consent. But the basic principle embodied in the GDPR – that market-based reforms can in themselves be radical, given how *radically distorted* existing platform markets currently are – is important.

That said, even the GDPR's principles may not go far enough. Let us restate what is needed here. Better market functioning requires that platform corporations and others in the consumer internet sector were required to offer users more optionality – including transparent options about how personal data will be used and shared, opt-in functionalities to all data collection and use, and perhaps most critically, *an option to share no behavioral data at all with the platform service while still having the opportunity to use it* – as was suggested by the German Bundeskartellamt in its case regarding Facebook's alleged use of its dominant market position in social media to force exploitative terms of service agreements on the company's users.[50] Indeed, this could be implemented through an *opt-in* regime for data collection, whereby the platform gathers personal data *only* in those cases where the individual consumer has expressly stated that the platform can do so – and *without the threat that, if they do not do so, they cannot enjoy the service.* Given that in contemporary societies there are no public alternatives for the sorts of services provided by, for example Facebook, this option – to use the service without surrendering data – is essential. This adjustment of platforms' terms of service is especially important given the lack of alternative forms of social connection at this scale, whether public or otherwise. A predictable criticism of this proposal is that it would disable the platform from generating sufficient revenue from the

[50] Cathryn Schaer, "Inside the German antitrust plan to destroy Facebook's data monopoly," *WIRED*, 13 June 2019.

consumer. but this argument does not hold. While there is no doubt that short-run profitability of a marginal consumer might decrease, and that associated costs might increase, the platform firms dominant in the democratic digital ecosystem today would likely maintain their dominance as they already possess a stranglehold over our aggregate attention. Profit margins might diminish substantially,[51] but from that retained customer attention the platforms could still generate significant revenues, albeit with less-precise targeting of ads and less-precise curation of content in individual social feeds: their marginal costs for adding extra users would still remain low. The benefits, though, are clear: we would have a more equitable, less biased digital media ecosystem that is far less reliant on monetizing our individualities and distorting the world as it appears to us.

This is precisely the approach advanced by the Bundeskartellamt (i.e., the German Federal Cartel Office), which noted that the forced deal – the transfer of large amounts of personal information from individual to corporation as the price of use of the firm's platforms, as noted in our earlier discussion of price-inelasticity – was exploitative.[52] This was the first attempt at a regulatory intervention that connected the practice of large-scale data collection and the problem of extreme market concentration. Though the Bundeskartellamt's charges have been challenged by Facebook[53], the underlying argument of the German regulatory body stands: there is at the heart of the consumer internet a dynamic of market power and information asymmetry that *forces* the consumer to part with her personal information including sensitive behavioural data in order to fully participate in society today. We must protect the individual from such overweening economic power.

Algorithmic Transparency

The modus operandi of the consumer internet corporation is to sweep up as much data – personal and proprietary – as possible and extract from it maximal profit from the digital "masses": its billions of users around the world.

In their commercial imperative to employ the user base's personal data to profile individuals and manipulate their media experience so as to maximize returns, corporate platforms induce algorithmic bias. Indeed, the core purpose of machine learning algorithms, throughout the consumer internet (whether we look at Google's ad

[51] For brevity, we are abstracting here from the details of particular platforms' business models.

[52] 'Bundeskartellamt prohibits Facebook from combining user data from different sources', Bundeskartellamt, 7 February 2019.

[53] Marc Wiggers et. al., "German Competition Authority Suffers Defeat In Landmark Facebook Case," *Lexology*, 29 August 2019.

personalization methods, Facebook's Audience Network and Lookalike Audiences, or the Twitter feed) is *to discriminate*: to assert that one person belongs in group A while the next belongs in group B, in order to determine visible segmentations within its user population. These inferences, if developed with confidence, are like virtual gold for the platform firm. Corporations that build algorithms and the demographic inferences they make possible will work to create the best environs *for such algorithms* – and correspondingly the best circumstances for propagating these forms of commercial bias. All this without even considering the egregious cases of algorithms reproducing race, gender and other forms of bias.[54]

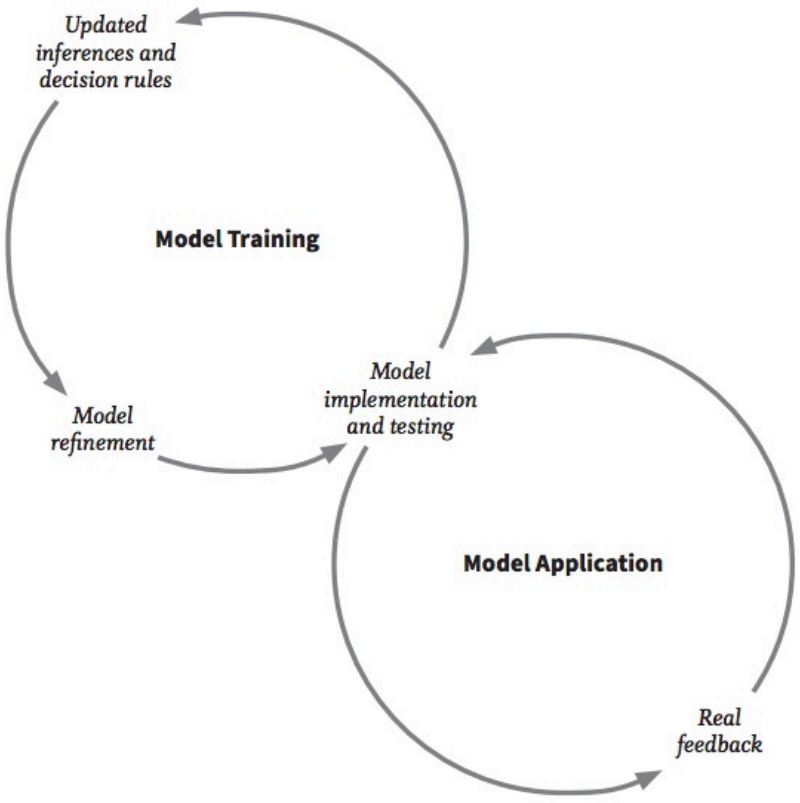


Figure 4. **The application of machine learning over the consumer internet**. Consumer internet platforms continually refine highly sophisticated machine learning models used to behaviorally profile consumers, segment them into countless audience segments, curate their social content, and target ads at them.

[54] Safiya Umoja Noble (2018) *Algorithms of Oppression,* New York University Pres; Virginia Eubanks (2018) *Automating Inequality,* St Martin's Press; Meredith Broussard (2019) *Artificial Unintelligence,* MIT Press; Ruha Benjamin (2019) *Race After Technology,* Polity;

Given this commercial imperative of generating bias for profit, it follows that the consumer internet industry allows, or even facilitates, activity that is harmful and at times indeed nefarious. There are clear red lines that should apply here. The United States of America has civil rights laws and federal election standards, for instance, and atop this are corporate policies that each of the dominant digital platforms has promulgated around topics like coordinated disinformation and online hate speech. And yet time and again we have seen content of that sort rise to the top of our social feeds and go viral. Because of the profit incentive inherent behind digital media – which is massive given the margins experienced in this industry – consumer internet platforms constantly approach the red lines of what is socially acceptable, and very often exceed them: for machine learning is blind to such red lines. Most often, these overreaches are likely not even intelligible to the public, since their actual operations are hidden behind closed doors.[55]

Transparency can begin to defeat the harms of this sort – transparency over the data held by firms and transparency into the algorithms developed and advanced by them to manipulate our media experience. Transparency can begin to rebalance the information asymmetry that is the core feature of the dynamic between the corporate and the consumer, and offer the individual a lens into the decision-making conducted by consumer internet platforms.

Transparency has been attempted in various forms, however with little success thus far. For years now, dominant consumer internet platforms have published so-called transparency reports in response to various corporate commitments and developments in regulatory policy. But these reports do little for the individual or critic keen to understand precisely the mechanisms by which dominant digital platforms manipulate how we experience the social world.

What the public demands is *comprehensive transparency*. This is what might have been offered by the Honest Ads Act, a bill introduced in the U.S. Congress by a bipartisan group of senators and sadly not passed, which would have imposed transparency over the provenance and funding behind any political digital advertisement, and regulated that digital platforms maintain a public database showing the political advertisements that they have hosted. Some activists have suggested that similar transparency standards should be applied to *all* digital advertisements – not only political ones. Though this would exempt firms from the discomfort of having to decide what ads are

[55] Frank Pasquale (2015) *The Black-Box Society,* Harvard University Press.

political and which are not, it would also eliminate in large part the information asymmetry from which the firms currently benefit.

We would suggest, however, that policymakers consider the possibility of going one step beyond this: by imposing a transparency regime, enforced by government-sanctioned entities that have the public's trust, to monitor all aspects of the internal workings of the dominant consumer internet platforms. Major consumer internet platforms have not only a dominant position in the industry, but a dominant presence in our lives and specifically our media consumption. Platforms present more and more consumers with the media content they see and, as such, they shape, far from view, our perspectives on the wider world, projecting an image of how the world is among our friends and family, our local and national politics, the economy. And yet there is no apparent commercial threat to the hegemony of Google and Facebook in their respective consumer-facing markets.

The resulting situation is one in which two corporations maintain private ownership over the definition of our collective experience. And yet there is a public-interest component to how we experience the world: as a public we need to see the world for what it is so we can deliberate over who we wish to be and what we wish to do. Protecting this public interest requires transparency over the types of personal data the dominant digital platform corporations collect on us, transparency over how they use it to profile us and keep us engaged on the platform, transparency over how they accept money for ad-targeting and how specific ad campaigns reach us over their platforms, and transparency over the ancillary algorithmic decisions they make to maintain a minimum of social order over their platforms. Going even further, we need a *radical transparency*[56] – overseen and enforced by government-sanctioned parties – over dominant internet platforms' business models to the extent that they interfere with the society and democracy we need.

Market Competition

Much academic, regulatory, and policy analysis has focused on the anticompetitive aspects of the dominant digital platforms. This is much-needed; jurisdictions like the United States and Europe possess important regulatory authorities to police anti-competitive behaviour in traditional industries.[57] Such frameworks should certainly be

[56] Dipayan Ghosh (2020), *Terms of Disservice* p. 233.

[57] We leave aside here recent arguments that shifting jurisprudential norms, particularly in the United States, have favoured a strict adherence to a narrowly interpreted consumer welfare standard, thus hampering regulatory efforts to punish much alleged anti-competitive behaviour.

brought to bear against digital firms where possible – though the novelties of the digital space have presented some uniquely difficult challenges for policymakers.

But our comment is broader. It is one thing to suggest that a firm is squeezing a bottleneck of economic activity it may possess control over, and that it is using that power to extract unfair rents out of the rest of society. It is entirely another to contend the already-dominant firm will organically tend toward growing market and social power because of the very nature of the consumer internet.

A tradition in antitrust enforcement is to ask oneself as a regulator of a monopoly firm that is perpetrating anticompetitive harms whether a breakup of the monopoly would facilitate the growth of a vibrant, dynamic industry of healthily competing firms – or whether such an outcome cannot be imagined even with breakup, requiring instead stringent and direct regulation of the firm to redistribute the balance of economic power away from it and back to consumers. If the former, one might employ Senator Warren's break-them-up logic. If the latter the regulator might acknowledge the "natural monopoly" nature of the firm as one that benefits from the organic generation of powerful barriers to entry and a powerful network effect – much like railroads or telecommunication networks, which in the United States possess regional monopolies.

While this remains an open question, we see evidence on both sides (the position of Google as a potential natural monopoly is perhaps clearer than that of Facebook). Resolving this is not the immediate issue. More important is to acknowledge that dominant digital platforms have indeed broken the norms on the traditional three counts: in hindering market innovation, raising the prices of their services as rendered to the rest of society, and diminishing quality of service. Something must be done urgently in response.

What we need is a regulatory framework to correct the market power problem at the heart of today's digital media ecosystem, which must include identifying and addressing the broader social and economic harms that market power problem generates.

Moderating Social Harms

In societies such as the United States of America, the regulatory path of least resistance means regulating the marketplace to see if this can settle the majority of the harms wrought by and through the consumer internet industry. Yet even to rebalance the marketplace requires, as we have just seen, bold, even radical, intervention. However, certain business practices need additional reform for overriding reasons concerning the

interests of a healthy society and a healthy democracy. Here, we focus on three core areas for such government intervention: content, data, and identity.

Reconsidering Platforms' Freedom from Content Liability

The American legal system maintains a powerful commitment to free speech, a framing that has affirmed through time a national predilection to protect individual civil liberties. The courts have, however, extended many of the rights appreciated by individuals to corporations over time, contending variously that corporations should maintain not only rights to property but also liberty, or as First Amendment scholar Adam Winkler writes, the "rights associated with autonomy, conscience or political freedom." Over time, the trajectory of jurisprudence has come to favor the interests of the business community at the expense, especially, of marginalized communities.[58]

This was not always the case. Winkler notes that over a century ago the "Supreme Court refused to grant corporations the right against self-incrimination," and that corporations once did not maintain a "constitutional right to spend money on elections." Though business interests did receive expanded protection, under Justice Lochner, the Supreme Court once drew a key distinction between property and liberty rights, on the ground that businesses should not maintain liberty rights as those latter rights were "protected by the Constitution only for 'natural, not artificial persons,'" as Winkler indicates. But a 1978 ruling contending that corporations had a right to channel money toward ballot-measure campaigns (as in California) followed decades later by the contentious *Citizens United v. Federal Elections Commission* ruling (of 2010) that businesses should have the same right as individuals to spend money on electoral campaigns effectively handed free speech protections to businesses almost as wide as those enjoyed by individual persons.

Many have warned of the deep harm that can be wrought by such a propensity to favour protection of speech liberties for the business community. Much of this advocacy has focussed around the protection of Section 230 of the Communications Decency Act, a portion of the U.S. Telecommunications Act of 1996 that effectively gives modern digital platforms - "interactive computer services" as defined in the law - freedom from liability over any user-generated content shared or otherwise disseminated over their platforms, although the same section also gives the platforms freedom to regulate content through censorship at their discretion.

[58] Adam Winkler, "Op-Ed: Corporations keep claiming 'We the People' rights. And they're winning," *The Los Angeles Times*, 2 March 2018.

To date, this issue has been approached as a problem of content moderation, but this is misconceived. Why? Because the sorts of offending speech including digital disinformation and hateful conduct online on which section 230 debates focus are largely *caused* by the business model at the core of the consumer internet on which we have focused in this paper: in particular, the practices of data collection for behavioral profiling and the resultant prioritization of engagement at the expense of all other considerations, which together drive profit margins for dominant digital platforms. It cannot be adequate therefore to leave platforms' legal liability in limbo – giving them an effective free pass for causing social harms - as does Section 230.

In prioritizing the profit interest, the dominant digital platforms actively distort the simple situation of a person speaking, for instance, into the public square (one of the basic situations for whose protection the First Amendment was designed initially). Platforms like Instagram and YouTube of course likely do not attempt to directly interfere with such ordinary free speech. But indirectly, in selectively promoting certain instances of speech over others and shaping the media that appears in our personalized social feeds in ways that best serve *their* profit interests, dominant digital platforms distort the traditional hierarchy and order of publicly accountable speech. This commercial-first behavior – driven largely by content-curation, behavioral profiling, and ad-targeting algorithms trained altogether to maximize returns – distorts the democratic baseline. And worse, dominant firms benefit precisely from that distortion of the democratic space because, as yet, there is no protection of the broader democratic interest.

Instead, digital platforms reshape our access to the public world in the profit interest, and through the same process generate social harms, without incurring liability. This situation cannot be allowed to continue. First, corporations do not require rights to free speech as humans do, as part of their basic liberty; at most corporations use such rights strategically in their business interests. Second, given those social harms to which platforms actively contribute, we would contend that at most Section 230 of the C.D.A. should offer dominant digital platforms protection from liability over *content generated when platforms operate as the medium for people to speak in a manner that does not impair the democratic process.* Where Section 230 gives platforms wider protection than this, it directly distorts the social world, and as such should be reformed.

We therefore propose that the U.S. Congress should consider targeted changes to Section 230 – amendments that would negotiate what is currently a blanket immunity for internet platforms by forcing liability over user-generated content in some cases and

specific contexts.[59] These proposed legal reforms are our attempt to establish new market norms that, while not necessarily restoring a mythical public town square, will help protect unimpeded public discourse and the democratic process.

- *Removing the liability exemption for commercial speech.* A substantial distinction between traditional media and the modern digital landscape is the mechanism by which marketers can access audiences with commercial messaging. There has emerged a strong commercial alignment between the interests of the dominant digital platforms and those of the marketers advertising over those platforms: both wish to engage the user with targeted advertising as much as possible, the platform in the profit interest and the marketer in the interest of influencing the consumption choices or other decision-making of the individual. Influence of course has been exercised before via media, for example television and radio broadcasting but for traditional media, content is publicly available and there is no algorithm at play that opaquely personalizes the user experience. As argued earlier in the paper, this and the general business model of the consumer internet is what has contributed to many of the negative externalities that we witness today, and transparency in and of itself cannot resolve the harms. Advocates have variously proposed, in response, a carve-out from Section 230 in the case of digital targeted advertising[60] – a proposal that we would endorse.

- *Placing checks on mass communication*. It is often the case that the most offending forms of content on dominant digital platforms are content that has been seen by a vast many people. It is well understood that content which is hateful, violent, false, or conspiratorial in nature tends to be consumed by users more readily than verifiable and relatively benign content – including, for instance, run-of-the-mill daily news. Scholars have, for instance, shown recently that "fake news" – including misinformation and intentional political lies – travels faster and farther than the truth.[61] As such, we would suggest that Congress consider carving out from Section 230 content that qualifies – in terms of level of consumption by unique individual users – as mass communication. Such a carve-out will have the effect of dampening platforms' incentive to help, through their algorithmic processes, viral content get generated.

[59] Parallel proposals are currently being developed within the European Community via the proposed European Digital Services Act.

[60] John Bergmayer, "How to Go Beyond Section 230 Without Crashing the Internet," *Public Knowledge*, 21 May 2019.

[61] Souroush Vosoughi, Deb Row and Sinan Aral (2018) "The Spread of True and False News Online", *Science,* 359: 1146-1151.

- *Adhering to criminal law*. Another situation to be discussed is where digital platforms facilitate the perpetuation of what could be illegal conduct – for instance, through enabling breaches of established U.S. civil rights laws established. For instance, the American Civil Liberties Union has highlighted in recent years the potentially wrongful unfairness of certain advertising mechanisms available over digital advertising platforms like Facebook's that have enabled the targeting and, conversely, the exclusion of certain audience segments according to protected class categories like race. A particularly contentious instance was highlighted in the case the U.S. Department of Housing and Urban Development brought against Facebook, noting that the company's enablement of targeting and exclusion of certain disadvantaged communities constituted a civil rights violation. Digital platforms have generally responded that as 'neutral' platforms, they only host content including advertising and the marketer's channeling preferences for that advertising. And yet, such behavior might constitute harmful, willful ignorance. In removing the liability shield for civil rights violations – in both advertising and organic contexts – digital platforms can more effectively be held accountable in those instances in which their business model works, directly or indirectly, to facilitate the spread of harmful content.

The crucial context for these reforms is the distinctive features of online social space that we outlined at the beginning of the paper. In online platforms, there is less accountability for what is said; there is every chance of unaccountable, inexplicable, unvetted, and potentially toxic virality; and perhaps most critically, there is a profit-minded corporation that sits behind the forum determining what gets seen by whom, guided by whatever content will optimize saleable ad space and the volume of collected personal data, rather than reflecting the democratic and public interest. These are the facts we must consider in reforming the social media ecosystem.[62]

Some might suggest that these impositions would be too taxing for small firms including start-ups to adhere to: we therefore suggest they apply only to dominant digital platforms that meet a hypothetical threshold in both users and average user attention rates. Congress could furthermore explore a gradated approach by which some more moderate regimes exist to treat firms that are neither fledgling nor market-dominant.

A perhaps sharper critique might be that digital platforms would over-compensate to comply with any such set of policies – preferring over time to moderate (through take

[62] See, e.g., Cass Sunstein (2017) *#Republic: Divided Democracy in the Age of Social Media,* Princeton University Press; and Whitney Phillips (2015) *This is Why We Can't Have Nice Things*, MIT Press.

downs or demotions) not only content that is clearly socially unacceptable, but also that which comes close to the red lines notionally established through implicit (or explicit) societal norms. This critique may, however, ignore the reality that firms in the digital ecosystem – in principle and in some respects - compete over attention; those that (for instance) censor particularly engaging content that approaches the red lines set by society but does not exceed them will necessarily be leaving engagement, and high-margin advertising revenue, on the table. In a market system, there exists some incentive for the digital media platform to strike the right balance and avoid such over-moderation, even if a perfect flow of information is impossible.

Data that Should Never be Gathered

A functioning system of privacy protection enables the consumer and citizen to protect *their own* interests: it is not a license for general state intervention in free speech. To state this another way, normatively, commercial data privacy is principally a system by which individuals detail their preferences to their service providers with full information, access, and knowledge, and their service providers enforce those preferences as data fiduciaries[63] of a sort. And yet there are areas that deserve a more robust form of protection in the interest of democracy. One relates to how platforms put to use the consents they obtain from consumers; the other relates to cases where genuine consent is not deemed possible.[64]

We propose, first, that digital firms can collect *any* form of information pertaining to an individual that the individual has fully consented to within a balanced economic exchange (that is one where consent is not forced by, for instance, the threat of withdrawal of service), but *only in so far as* that information is functionally necessary for the service: go beyond that, and the data being asked for goes beyond the ambit of the economic bargain being struck.[65]

Second, we propose that there may be certain types of data that policymakers should consider prohibiting them from collection and use entirely. Such forms of information might include anything that is particularly sensitive. This is an area where a much fuller debate is needed, so our proposals are intended only as starting-points, but they already build on debate that has been emerging. At a minimum we would suggest that this might

[63] Jack Balkin (2016) "Information Fiduciaries and the First Amendment," *UC Davis Law Review,* 49: 1183-1234.

[64] Elettra Bietti (2019) "Consent as a Free Pass: Platform Power and the limits of the Informational Turn" (available via SSRN); Nancy Kim (2019) *Consentability: Consent and its Limits.* Cambridge University Press.

[65] We follow here the idea outlined in the Fair Information Practices. (See Secretary's Advisory Committee on Automated Personal Data Systems, "Records, computers, and the Rights of Citizens," *U.S. Department of Health, Education and Welfare.*)

apply to data pertaining to activity *within the home* (beyond what was strictly necessary, for example, to the service functioning that the user aimed to purchase), or pertaining to a *facial recognition* metric, or that data generated through use of *biometric devices* might constitute sensitive information that is unique and highly revealing. Such data extraction should receive independent scrutiny through entities that have the public's trust as to whether they belong in the consumer internet ecosystem at all.

Such bans – or any imposition of principles of a lower order of regulation – would need to be strictly monitored, with a periodic review of performance, after which evidence of continued inappropriate intrusions to personal autonomy might generate permanent regulation or an outright ban of certain practices.

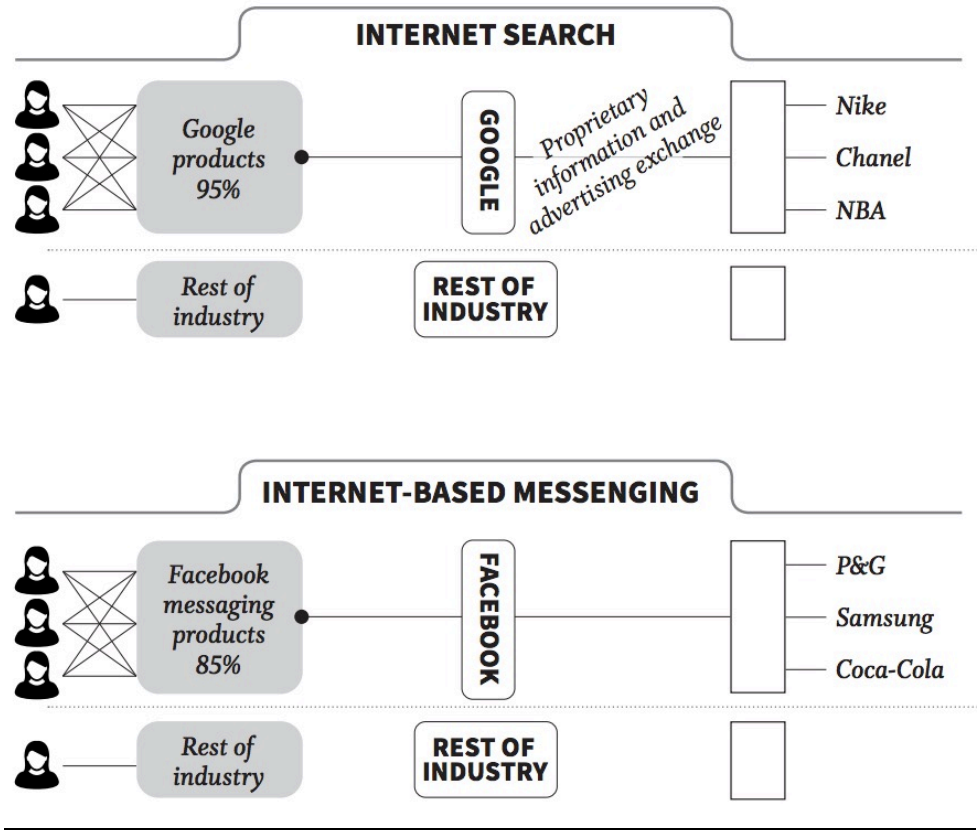


Figure 5. **Two-sided platform monopolies**. Consumer internet platforms engage two primary markets: advertisers and end consumers. It is in the latter that the dominant platforms possess respective market monopolies through which they rake from consumers a novel form of digital currency that is a complex combination of data and attention at a monopolistic rate. This value is translated through proprietary systems of exchanges to the other market – in the face of digital advertisers – for transfer into monetary value.

Anonymity as Conditional Privilege

At the paper's start, we mentioned online anonymity, and the incentives it generates for offensive online speech, as a difficult issue in regulating the online social sphere. We return to this point now.

We would suggest that the regulatory community consider measures requiring the disclosure of real identities on dominant consumer internet platforms under certain strictly defined circumstances. Though as a general matter we defend the principle of anonymity as a protection for vulnerable actors that allows them the opportunity to speak safely and freely,[66] it could be made conditional[67] – such that all platforms that openly enable users to remain anonymous must *remove that anonymity* from an offending user in the event of the breach of terms and conditions regarding abusive speech, threats to violence, and disinformation. More than that, if the platform fails to remove anonymity to offenders, the platform itself should lose *its own* right to support anonymity. This provision would apply to all platforms, not just large or well-established ones.

Imposing this requirement need not impede the First Amendment; such a regulation could be framed in terms of protecting society against what publicly trusted and sanctioned entities regard as the harshest and most damaging content online.

Conclusion

We have shown, in broad outline, how underlying all of today's debates about the online public sphere is a profound shift in how the social world is configured: a transformation which grants to profit-oriented corporations a new power to shape the infrastructures, architectures and spaces of social life, causing a profound misalignment. This transformation poses challenges for the regulators of markets, but also for regulators of technology concerned to protect the good of society and democracy. That challenge has barely been defined, let alone met.

This challenge emerged from technological and legal developments,[68] many of which were not originally introduced with such a profound social transformation in mind. But the direction of travel – towards a public world profoundly molded around commercial, not

[66] Citron *Hate Crimes*, 221ff.

[67] Citron op. cit. 239.

[68] See Cohen *Between Truth and Power,* for an excellent account of the legal adjustments and regulatory permissions which enabled the technological changes described earlier in this paper to acquire everyday force.

public, imperatives – was predicted two decades ago,[69] even if then the dangers were at most potential. Now those dangers are real, since for 15 years platform corporations have implemented a business model that aligns optimally the interests of platforms and advertisers with those of content providers, whether or not the latter are driven by anti-social goals. Platforms manage the terms of that business model which, to date, has not been challenged by regulators. The result is a giant machine for generating social harm. Today's online public world of unprecedented vitriol, abuse, instability and weak deliberation constitutes the wreckage left in the wake of that machine's progress.

A realignment of the digital social world is needed to address this challenge. It requires decisive action that uses existing regulatory tools to the full, and designs new ones, as part of a regulatory reset for the internet.

That realignment has two sides. First, market reform, which restores to the market situations now dominated by digital platforms effective forms of protected privacy, enabling individuals to exercise real choice about how data that relates to or affects them is gathered, processed, and used: such market reform will strike at one key way in which the internet's business machine generates social harm, reducing its momentum, while also enabling markets to work better.

But such market reform cannot be sufficient, at least in the medium term, to address the negative social externalities of the consumer internet. We need a second side of the digital social contract, which imposes radical transparency on platform corporations by uncovering the so far uncontrolled social harms from which they profit. Platform corporations should be required to take urgent remedial action against controllable social harms, unacceptable data collection, and unregulated anonymity: those proposals in turn require adjustments to platforms' current blanket immunity from responsibility under Section 230 of the Communications Decency Act. If platform corporations fail to take such remedial action, as required by regulators, further more drastic measures against the social harms associated with the consumer internet's business model, such as platform break-up, should be contemplated.

If pursued, this regulatory reset for the internet has the chance of halting, even reversing, the damage that two decades of unregulated social design have caused to our societies – and our democracies. The complex deliberations and negotiations required to achieve this digital realignment will be a small collective price to pay, compared with the benefits from success. Such success would mean that, for the first

[69] Paul Schwartz (2000), "Internet Privacy and the State".

time, in the United States of America and elsewhere, the consumer internet would start functioning as a *citizens' internet* that supports, rather than undermines, the foundations of democratic life.

Acknowledgements

The authors thank Paul Barrett, Joshua Geltzer, John Haigh, Karen Kornbluh, Robin Mansell, Robby Mook, Asad Ramzanali, Anya Schiffrin, Ben Shields, Ramesh Srinivasan, and José van Dijck for generously offering to review this paper and for providing feedback on the merits of the findings and policy arguments herein. The authors also thank Victoria Groves-Cardillo and Scott Leland for their guidance, as well as the Harvard Kennedy School's Mossavar-Rahmani Center for Business and Government and the London School of Economics and Political Science's Department of Media and Communications for their generous support of this scholarship.

Author Biographies

Dipayan Ghosh, Ph.D.

Co-Director, Digital Platforms and Democracy Project & Fellow, Mossavar-Rahmani Center for Business and Government

John F. Kennedy School of Government
Harvard University

Dipayan Ghosh is the co-director of the Digital Platforms & Democracy Project at the Harvard Kennedy School and lecturer of law at Harvard Law School. He is the author of *Terms of Disservice* (Brookings). Ghosh served as privacy and public policy advisor at Facebook, and prior was a technology and economic policy advisor in the White House during the Obama administration. His work on AI, privacy, disinformation, and internet economics has been cited and published widely, including in *The New York Times, The Washington Post, The Wall Street Journal, HBR*, *CNN*, *MSNBC*, *NPR* and *BBC*. Named to the *Forbes 30 Under 30*, he received a Ph.D. in electrical & computer engineering from Cornell and an MBA from MIT.

Nick Couldry, Ph.D.

Professor of Media Communications and Social Theory & Faculty Associate, Berkman Klein Center for Internet and Society

London School of Economics and Political Science

Nick Couldry is a sociologist of media and culture. He is the author or editor of fifteen books including *The Mediated Construction of Reality* (with Andreas Hepp, Polity, 2016), *Media, Society, World: Social Theory and Digital Media Practice* (Polity 2012) and *Why Voice Matters* (Sage 2010). His latest books are *The Costs of Connection* (with Ulises Ali Mejias, Stanford UP 2019), *Media: Why It Matters* (Polity 2019), and *Media Voice Space and Power: Essays of Refraction* (Routledge 2020). He jointly led, with Clemencia Rodriguez, the chapter on media and communications in the 22-chapter 2018 report of the International Panel on social Progress: www.ipsp.org. From 2014-2017 he was Chair of the Department of Media and Communications at LSE.