8

Why It Is So Difficult to Regulate Disinformation Online

Ben Epstein

Efforts to strategically spread false information online are dangerous and spreading fast. In 2018, a global inventory of social media manipulation found evidence of formally organized disinformation campaigns in forty-eight nations, up from twenty-one a year earlier.[1] While disinformation is not new, the ways in which it is now created and spread online, especially through social media platforms, increase the speed and potency of false information. As a report from the Eurasia Center, a think tank housed within the Atlantic Council argues, "There is no one fix, or set of fixes, that can eliminate weaponization of information and the intentional spread of disinformation. Still, policy tools, changes in practices, and a commitment by governments, social-media companies, and civil society to exposing disinformation, and building long-term social resilience to disinformation, can mitigate the problem."[2] In other words, false information purposefully spread online is actually a series of major problems that require an all hands on deck approach.

The 2016 election and the revelations in the years since about the breadth of disinformation have opened many eyes to the potential impact of strategic dissemination of false information online.[3] As this complex problem has gained greater attention, proposed interventions have spread at 5G speed. Heidi Tworek correctly notes in her chapter that five years ago there was a question about whether social media was going to be regulated. Today, that question has morphed into how and when. Tworek uses historical examples from Germany to provide greater context for the current disinformation age and outlines five historical patterns that create the structural conditions that enable disinformation. First, disinformation

https://doi.org/10.1017/9781108914628.008 Published online by Cambridge University Press

is a part of information warfare, which has been a long-standing feature of the international system. She argues that if the causes of disinformation are rooted in international causes, some of their solutions must also be international in design. Second, physical infrastructure matters. The architecture of political communication spans a hybrid media system that includes traditional media along with digital forms, all of which have been used extensively for coordinated disinformation.[4] Online disinformation is a strategy disseminated by the very infrastructure of the Internet and effective regulation of disinformation requires an understanding of the organization and control of that infrastructure. Third, business structures are more important than individual pieces of content. In other words, as the main sources of information, those companies with market dominance must be understood as fundamental to the form of the disinformation Fourth, regulatory institutions must be "democracy-proof," with clarity of purpose, a long-term view allowing room for innovation, and structural guards against any takeover by those who would use such tools to increase disinformation for their own ends. Fifth, media exploit societal divisions, and it is these divisions that fuel so much of the disinformation spread online.

Disinformation is neither a new problem, nor a simple one. This chapter aims to build on Tworek's historical patterns and apply them to the modern disinformation age in order to clarify the challenges to effective disinformation regulation and to offer lessons that could help future regulatory efforts. This chapter identifies three challenges to effective regulation of online disinformation. First, the question of how to define the problem of disinformation in a way that allows regulators to distinguish it from other types of false information online. Second, which organizations should be responsible for regulating disinformation. As Tworek notes, the international nature of online disinformation, the physical structure of the Internet, and the business models of dominant online platforms necessitate difficult choices regarding who should be in control of these decisions. Specifically, what regulatory role should belong to central governments, international organizations, independent commissions, or the dominant social media companies themselves. Finally, we must ask what elements are necessary for effective disinformation regulation.

After analyzing the major challenges, four standards for effective disinformation regulation emerge. First, disinformation regulation should target the negative effects of disinformation while consciously minimizing any additional harm caused by the regulation itself. Second, regulation

should be proportional to the harm caused by the disinformation and powerful enough to cause change. Third, effective regulation must be nimble, and better able to adapt to changes in technology and disinformation strategies than previous communication regulations. And fourth, effective regulations should be as independent as possible from political leaders and leadership of the dominant social media and internet companies and guided by ongoing research in this field as much as possible.

CHALLENGE 1: DEFINING THE PROBLEM

Terminology and definitions matter, especially as problems are identified and responses are considered. Disinformation is one of a few related, and often confused, types of false and misleading information spread online. There are many types of misleading information that can be dangerous to democratic institutions and nations. A number of recent studies have attempted to identify the definitional challenges associated with false or misleading information online in order to produce useful definitions for the purpose of more clearly understanding the problem.[5] There are two axes upon which inaccurate information should be evaluated: its truthfulness, and the motivation behind its creation.[6] False information falls into two broad categories, disinformation and misinformation, depending on whether the information was spread intentionally or not. This paper uses the definitions from Claire Wardle's essential glossary of the information disorder, which was also adopted by the High Level Expert Group (HLEG) on disinformation convened by the European Commission:[7]

Disinformation: false information that is deliberately created or disseminated with the express purpose to cause harm or make profit.

Misinformation: Information that is false, but spread unintentionally and without intent to cause harm.

While helpful, these two baskets encompass a wide variety of information, only some of which have led to calls for greater scrutiny and regulation. The hodgepodge of terms and uses have been described as information disorder.[8] Wardle describes seven different types of mis- and disinformation and offers a matrix that details types of false information (satire, misleading, manipulated, fabricated, impostor, false, etc.), the motivations of those who create it (profit, politics, poor journalism, passion, partisanship, parody, etc.), and the different ways that the content is disseminated (human vs. bot).[9] Put simply, there is a need to recognize the difference between the false and misleading information

spread by Russian troll farms meant to influence the 2016 election, and satirical articles from *The Onion*.

The definitional challenges to creating effective regulation aimed at misleading and harmful information are further complicated because the term that has captured the popular imagination is nether misinformation, nor disinformation. It is *fake news*. Hossein Derakhshan and Claire Wardle document the dramatic increase in the use of the term fake news by politicians, the public, and scholars alike, especially since the 2016 election.[10] The increase in attention paid to fake news coincided with President Trump's weaponizing of the term.[11]

Fake news may be the catch all phrase that has recently rung alarm bells the loudest, however, it cannot effectively be applied as the definitive realization of false information online because of its variety of forms, definitions, and uses. Fake news is a term that is great for clickbait but terrible as a target for effective regulation. It is a confusing and overly broad term that should be minimized in academic work and should not be used in any thoughtful discussion of regulatory efforts.[12]

Disinformation is the appropriate term for issues arising from intentional and harmful false information and is better suited for regulatory laws and legal action, because those responsible can potentially be identified. Disinformation can take many forms and may be conducted for economic or political gain. An example of disinformation for economic gain was the pro-Trump disinformation campaign spread by students in Veles, a town of 55,000 people in the country recently renamed North Macedonia; a campaign which was not ideological but instead was purely based on which messages received the most clicks and attention.[13] Politically motivated disinformation can target electoral results or other sociopolitical outcomes like the efforts by the Myanmar military to support a horrific ethnic cleansing campaign against the Rohinga, a Muslim minority group. For over half a decade, members of the Myanmar military conducted a disinformation campaign on Facebook which targeted the Rohinga, and paved the way for brutal attacks, persecution, and rape, all on a colossal scale. The disinformation campaign was particularly effective because Facebook is so widely used in Myanmar, and many of its 18 million internet users regularly confuse the social media platform with the Internet itself.[14]

The High Level Expert Group (HLEG) assembled by the UN, helpfully described how disinformation

includes forms of speech that fall outside already illegal forms of speech, notably defamation, hate speech, incitement to violence, etc. but can nonetheless be harmful. It is a problem of state or nonstate political actors, for-profit actors, citizens individually or in groups, as well as infrastructures of circulation and amplification through news media, platforms, and underlying networks, protocols and algorithms.[15]

Disinformation can take many forms and is linked to a varied group of actors who create it, and a variety of platforms which are used to disseminate it. However, disinformation is always perpetuated on purpose by a particular group of responsible actors and has potential to cause harm. Recognizing these consistent traits serves as the starting point for any effective regulatory action.

CHALLENGE 2: WHO SHOULD BE IN CONTROL OF THE REGULATION?

Regardless of the specific goals of effective regulation, the practical nature of implementation must be addressed. That involves determining who should do the regulating, and if regulation is actually necessary at all. Any regulation must be for a particular purpose. Traditionally, regulations are put in place to protect or assist a population or a group within a population, and that need is clearly present here. Concerns about various types of false or misleading information online and the need to address them are widespread.[16] When it comes to combating disinformation, there are three main options that have been internationally adopted: no regulation, self-regulation by industry leaders, or government regulation.

A system of minimal or no regulation is the starting position for many nations in the Western world, and is supported by free-market arguments about the benefits of letting the consumers and corporations make the decisions on both efficiency and ethical grounds. It is also articulated by a wide variety of lawyers, technology experts, media companies, and free speech campaigners, who have argued that hastily created domestic measures outlawing disinformation efforts may prove ineffective, counterproductive, or could manifest themselves as thinly veiled government censorship.[17]

Often an opposition to government regulation or action is coupled with a push to empower individuals and the public at large to develop skills to improve their digital literacy, in order to be better prepared when they encounter false information online.[18] Research into media and digital

literacy is extensive and a number of important studies have specifically focused on understanding how we can identify and minimize the effects of false information online, especially when encountered on social media.[19] However this is all directed at helping people become better able to identify misinformation. As stated earlier, disinformation is much better suited for regulatory action because it is effected with intention and as such, there are groups or individuals who are responsible.

Government Regulation

The fight against online disinformation campaigns requires systematic interventions, and governments are often identified as the organizations with the size and resources to address the scale of the problem. Government regulation can take on many forms and, as of early 2019, forty-four different nations had taken some action regarding various forms of false information online. However, only eight of these nations had even considered actions specifically aimed at limiting harmful disinformation originating from either inside or outside the country.[20]

Governments are also notoriously slow to respond to complex problems, especially those involving newer technology, and the government response to disinformation is no different.[21] Nearly three years after the 2016 US election, which featured a massive and successful disinformation campaign run by the Russian government to influence the election in favor of Donald Trump, the US Defense Department announced a program that aims to identify disinformation posts sent on social networks in the USA moving forward. The Defense Advanced Research Projects Agency (DARPA) will test a program that aims to identify false posts and news stories which are systematically spread through social media at a massive scale. The agency eventually aims to be able to scour upwards of half a million posts, though the rollout will take years and will not be fully functional until well after the 2020 election, if ever.[22] Relative to the speed of innovations in technology and disinformation strategies, the proposal put forth by the US Department of Defense moves at a glacial pace.

Beyond efficiency concerns, another daunting challenge to effective government regulations is finding the right balance between the expertise needed to regulate today's complicated, hybrid media environment and the independence from industry leaders needed to create policies that are as objective as possible.[23] There is a long history of industry leaders influencing communication policy and regulations. In the American context, the Federal Communication Commission (FCC)

https://doi.org/10.1017/9781108914628.008 Published online by Cambridge University Press

and the Federal Radio Commission (FRC) were both heavily influenced by industry leaders, as were many efforts at internet regulation over the past decade, such as net neutrality decisions. Perhaps this should not be surprising when we realize how many of the members who have served on the FCC over the past eighty-five years came from careers working for the companies they were then asked to regulate.[24] Nevertheless, government policies and actions often have unparalleled legal, economic, and political force, and have the potential to create the most sweeping and lasting changes.

Action taken at a national or even regional level, like the EU, may be insufficient to tackle many challenges caused by disinformation for a number of reasons, not the least of which is the fact that political parties in many nations are aligned with movements spreading disinformation and hate speech, and any new government standards run the risk of being branded as repressive and politically motivated by these politicians and their supporters. This governmental role is further complicated by the international nature of disinformation that Tworek describes.

In one tragic example, days after members of the Sudanese military massacred a number of pro-democracy protesters in Khartoum in June 2019, an online disinformation campaign emerged from an unlikely source, an obscure digital marketing company based in Cairo, Egypt. The company, run by a former military officer, conducted a covert disinformation campaign, offering people $180 per month to post pro-military messages on fake accounts on Facebook, Twitter, Instagram, and Telegram. As investigators from Facebook pulled at the string of this company, they discovered that it was part of a much larger campaign targeting people in at least nine nations in the Middle East and North Africa, emanating from multiple mirror organizations existing in multiple countries. Campaigns like this have become increasingly common, used both by powerful states like Russia and China, and smaller firms, aimed at thwarting democratic movements and supporting authoritarian regimes.[25]

This recent Sudanese case involves every one of Tworek's historical patterns, and begs the question: what form of regulation could best limit the harmful effects of these anti-democratic disinformation campaigns? In this case, the platforms used to post messages were central to the campaign, and therefore such platforms must be included in either externally enforced self-regulation, in the mode of the EU Code of Practice on Disinformation, or in traditional regulation that has the power to impose fines and penalties.

Internet infrastructure, communication, commerce, politics, and false information all extend beyond borders, yet decisions about policies and regulations are often national in origin and enforcement. For over two decades, scholars have explored the jurisdictional complexities of internet regulation.[26] While there are exceptions, such as the high level group organized by the EU, and longstanding efforts by the Internet Corporation for Assigned Names and Numbers (ICANN), most internet regulation is national, and many nations hold different cultural, political, and ethical positions regarding if, when, and how to regulate.[27]

There are a wide variety of positions about whether or not the government should actively regulate what is or is not true online. However, there is no question that the problem is pervasive. The 2018 Digital News Report found that a large portion of citizens across the world had been exposed to information in the week preceding the survey that was completely made up, either for political or for commercial reasons.[28] But there is a wide discrepancy in how people around the globe feel about the role of governments in fighting misinformation.[29] It is widely understood that privacy rights have been valued more highly than the roles of content providers in places like Europe, but less so in America. These values have helped to shape different government actions regarding the Internet more broadly, and online disinformation in particular.[30]

The First Amendment has been a consistent source of resistance to media regulation throughout American history, especially for content creators. While the protections of the First Amendment have extended much more broadly to print media than broadcast, the Internet has generally been regulated lightly. Beyond the First Amendment protections, any interventions that aim to regulate content creators or internet service providers (ISPs) will confront the long-standing legal protections provided by Section 230 of the Communications Decency Act of 1996 (CDA 230). CDA 230 is a key legal provision which broadly shields platforms from legal liability for the actions of third-party users of their services, and it has been seen as a cornerstone supporting free expression on the Web. CDA 230 has also been used to inhibit platform responsiveness to the harms posed by harassment, defamation, child pornography, and a host of other activities online. Therefore, the escalating debates on how to address disinformation online will join a long history of efforts to reform or eliminate the shield provided by CDA 230.[31]

Though there are legal and constitutional challenges that inhibit government action in the United States, the decisions there will have a disproportional impact on the rest of the world. This is due to the fact

that the majority of major global content providers and social media platforms were founded and primarily operate out of the USA. Thus Facebook, Twitter, Google, Apple, and Amazon, all dominant global players, could be affected by actions taken in the United States. While each of these companies and platforms have been affected by regional or national policies in various parts of the world, the United States would have more authority than any other to force any structural change or to mandate action regarding disinformation online.

The Power of the Platforms and Self-Regulation

The physical infrastructure and business models that Tworek notes are often overlooked when it comes to the causes of disinformation and potentially effective regulations. This is exemplified by the small number of dominant platforms that act as the lungs of disinformation campaigns. These platforms have been designed to keep users interested, engaged, and logged on as long as possible through the use of sticky content. This content is supported by black box algorithms that drive the experiences of users, and must play a role in potential regulatory decisions. Algorithms are one of the most important curators of internet users' media intake in the modern hybrid media system.[32]

It has been shown that algorithms often steer users to extreme content, especially on Facebook and YouTube, two of the most prominent platforms used for spreading disinformation around the world.[33] One employee of Google-owned YouTube created a grouping of YouTube videos associated with the alt-right, a loosely connected right wing group in the USA that peddles misogynistic, nativist, white supremacist, Islamophobic, and anti-Semitic rhetoric, including conspiracy theories and disinformation campaigns. The grouping found that alt-right videos on YouTube were extraordinary in size and reach, comparable to music, sports, and gaming channels, and aided by algorithms.[34]

Some nations are trying different ways to reduce the power of these platforms. In some instances, nations are attempting to force platforms to counter the effects of their very successful business models. In March 2018, after the Cambridge Analytica scandal in which Facebook allowed the company to harvest tens of millions of users' data for "psychologic profiling" and use it for political purposes, Germany sought to stop the disinformation spread on Facebook. While the goal is a good one, the means that Germany took was to try to gain access to the black box that is the Facebook's algorithm. There are many concerns about this

approach. First, the legality of forcing Facebook to disclose their proprietary algorithm is far from a given. Second, it's unlikely that making such information more transparent would actually help Facebook users identify and avoid disinformation spread on their pages as much as other efforts, like making the funding of political ads on Facebook more obvious. Third, this approach is not targeted directly at disinformation. And finally, this effort could potentially be counterproductive as greater transparency of Facebook's algorithm could give greater power to those who would seek to create disinformation campaigns in the future.[35]

Government action often extends to related areas including limiting the size and reach of individual companies or their use of data, or protecting the privacy of users.[36] For instance, there have been increasing calls for the breakup of massive media companies like Facebook, Amazon, and Google.[37] In September 2019, official antitrust investigations were launched by multiple states into Facebook and Alphabet, the parent company of Google.[38] Meanwhile the FBI, the Department of Homeland Security, and the Director of National Intelligence have met with leaders from platforms like Facebook, Google, Microsoft, and Twitter to focus on national security issues on the platforms in connection to the 2020 election.[39] There is no question about the power of the dominant platforms. The only question is whether they will be in charge of self-regulation or if governments or internationals commissions will take the reins.

Self-Regulation

Mark Zuckerberg once stated that, "in a lot of ways Facebook is more like a government than a traditional company. We have this large community of people, and more than other technology companies we're really setting policies."[40] He was right. And this reality aptly describes other behemoth social media and internet companies like Google, Amazon, Apple, Microsoft, Twitter, WeChat, and Alibaba that play central roles in the spreading of information, fake or otherwise. Facebook and other content companies make and enforce polices about online content every day and the option of allowing, or aiding a self-regulatory approach is a path that many support. As the 2018 Digital News Report found, far more online news consumers prefer media or tech companies working to identity real and false news than governments.[41]

Self-regulation of internet content is far from a new option and has evolved with the growth of numerous institutions and self-regulatory

https://doi.org/10.1017/9781108914628.008 Published online by Cambridge University Press

systems over the past two decades.[42] One advantage of self-regulation is that media companies simply understand how they work best and are often motivated to provide effective self-regulation in lieu of potential government action that could be more disruptive of their services or business. There are also legal reasons in many nations as to why more heavy-handed government regulations are either more difficult or flatly illegal.

All of these considerations led the European Commission, the executive branch of the European Union, to adopt a standard policy-making path in addressing emerging issues that involve technological challenges, which was then used to create the EU Code of Practice (CoP) on Disinformation. The CoP on Disinformation was put into practice in early 2019, a few months before the EU parliament elections in May 2019.[43] Importantly, the EU CoP preferred self-regulation over traditional government-directed regulation to target and reduce disinformation at this stage because they saw it as faster and more flexible than traditional regulation, and they didn't see a tested top-down solution for the problem of disinformation.[44]

The options for control are not a binary choice between autonomous self-regulation by the powerful platforms themselves and legislation handed down by national or international governmental bodies. Independent commissions are likely going to play an important role in the regulation of disinformation moving forward because they can have greater impartiality from government or corporate control; can potentially act more nimbly than governments; and can have the authority to hold companies or individuals accountable. In March 2019, Mark Zuckerberg surprised some in admitting that their platform had too much control. He stated that he supported increasing regulatory action specifically aimed at protecting election integrity, privacy, data portability, and harmful content including disinformation. He also went further, promising to establish an independent group working within Facebook to help guide these efforts. In September 2019, Facebook unveiled its plans for a new independent board that could have the power to review appeals made by users and make decisions that could not be overruled, even by Zuckerberg. This Facebook "Supreme Court" is not focused initially on curbing disinformation on the platform, but could evolve into a larger board with multiple foci. Regardless, it serves as an example of a powerful independent group working within a company with broad authority to make and enforce reforms.

CHALLENGE 3: WHAT SHOULD EFFECTIVE REGULATION LOOK LIKE?

Regulation is often as tricky as it is controversial. Tworek offers extremely helpful, historically defined, guideposts for effective disinformation regulation. As she describes, effective regulation should be forward thinking, adaptable, clear in focus, and responsive to changes in technology and the international nature of both online communication and disinformation campaigns. Perhaps most challenging, effective regulation of disinformation should aim to protect the democratic ideals, structures, and nations that have been threatened, but should also remain "democracy proof" enough to avoid the takeover of regulatory efforts by powerful actors who would aim to use such tools through political means or otherwise, in order to further their disinformation goals. Therefore, it should remain vigilantly independent.[45] The stakes are as high as the difficulties faced.

Disinformation strategies and the digital tools and platforms that are used to spread it are changing quickly, yet regulatory action is notoriously slow. Margaret O'Mara, historian and expert on the history of the technology industry, sums it up well: "Technology will always move faster than lawmakers are able to regulate. The answer to the dilemma is to listen to the experts at the outset, and be vigilant in updating laws to match current technological realities."[46] Many of the most important regulatory frameworks governing the Internet today originated in the 1990s, when the Internet was a far cry from what it is today, and today's leading social media platforms and online disinformation campaigns were nonexistent.[47] It is important that regulations, though long overdue, are clearly targeted and proportional. Some nations, like Germany, have been quick to act. However, there are concerns that some of the early regulatory steps may be excessive and potentially ineffective.

Another concern is that the regulatory teeth are proportional to the harms found, and large enough to change the actions of the some of the most profitable and influential companies on earth. Recent instances in the USA, aimed at penalizing major platforms for past inaction, serve as a good example. After a spiraling investigation sparked by the Cambridge Analytica scandal, the Federal Trade Commission (FTC) levied a five-billion-dollar fine, its largest ever, on Facebook in July 2019. While large in absolute dollars, it is less than a third of the $16 billion-dollar profit Facebook earned in the second quarter of 2019 alone. It's also notable that, although the FTC considered a much larger fine along with the requirement for changes in Facebook's actions, both were scrapped

due to fears of a drawn-out court battle. Two months later, Google agreed to pay $170 million in fines to the FTC for violating the 1998 Children's Online Privacy Protection Act due to data collected from children by YouTube, a part of Google. Alphabet, the parent company of Google is set to make over $160 billion in profits in 2019, $20 billion of which will be generated by YouTube. A fine of $170 million is a drop in the bucket.[48] While neither of these regulatory actions are focused on disinformation, they are examples of how recent efforts to regulate internet companies and social media platforms over data or privacy issues are using outdated policy and ineffective penalties.

Thankfully, the work of providing thoughtful and comprehensive suggestions for effective policy aimed at disinformation has already begun. The most rigorous efforts so far have emanated from Europe. Wardle and Derakhshan produced one of the first of these efforts with their 2017 report for the Council of Europe which aimed to define the major issues involved in what they label "information disorder," and to analyze its implications for democracy and for various stakeholders.[49] They go on to offer suggestions for what technology companies, media companies, national governments, education ministries, and the public at large could do moving forward.

In November 2018, the Truth, Trust and Technology Commission from the London School of Economics and Political Science published a report called "Tackling the Information Crisis: A Policy Framework for Media System Resilience." In this report, the commission defined "five giant evils" of the information crisis that effect the public and should be targeted by thoughtful policy: confusion, cynicism, fragmentation, irresponsibility, and apathy. To fight against these evils, the report details short, medium, and long term recommendations for the United Kingdom which includes an independent platform agency, established by law, to do research, report findings publicly, coordinate with different government agencies, and to collect data and information from all major platforms and impose fines and penalties.[50] The foundation of solid research included in the commission report is an important place to start. While there is a lot of good scholarship on disinformation, there are research gaps that remain.[51]

A few months after the report, the UK government's Home Office and the Department for Digital, Media, Culture and Sport followed up these proposals in a white paper that called for a new system of regulation for tech companies aiming to prevent a wide variety of online harms including disinformation. The white paper outlines government proposals for

consultation in advance of passing new legislation. In short, it calls for an independent regulator that will draw up codes of conduct for tech companies, outlining a new statutory "duty of care" toward their users, with the threat of penalties for noncompliance including heavy fines, naming and shaming, the possibility of being blocked, and personal liability for managers. It notably describes its approach as risk-based and proportionate, though both are subjective.[52]

The white paper is a set of expectations for companies to follow that serve as guidelines for future regulatory action and codes of practice. However, any interventions aimed at fighting the harmful effects of disinformation must avoid creating more harm than they reduce. In particular, many groups have already voiced their concerns about the potential negative effects of regulation on innovation, and a slippery slope of censorship and free speech violations resulting from efforts to reduce the effects of disinformation.[53] The proof of harm caused by disinformation is not always clear-cut and the potential for major restrictions on free speech increases as subjective judgements are made. It is also not clear how to regulate problematic information spread with differing types of intentions, such as the anti-vaccination information spreading across the world like a disease, though without a clear economic or political motivation.[54]

THE LESSONS LEARNED FROM THE CHALLENGES OF REGULATING DISINFORMATION

The distance between thoughtful recommendations to combat disinformation and effective regulatory policies are vast due to political complications, divergent philosophies about the dangers and threats to democratic processes and ideals, and regional differences. In addition, online disinformation does not exist in isolation and is impacted by other concerns that have led many to call for reforms and regulation of issues including data security, privacy issues, and the oversized power and influence of platforms like Facebook and YouTube.[55] The EU General Data Protection Regulation (GDPR), in effect since May 2018, is a great example. The GDPR is arguably the most important change in data privacy regulation in decades and can impact disinformation efforts in a number of ways, notably by impacting platforms and companies that are used to spread disinformation.[56]

There are many reasons why regulating disinformation online is difficult, but the time for simply admiring the problem is over.[57] This chapter

https://doi.org/10.1017/9781108914628.008 Published online by Cambridge University Press

has detailed the complex challenges that face those who seek to design and implement effective disinformation regulations. The first set of challenges centered around the definitional challenges of distinguishing between misinformation and disinformation and why disinformation is ripe for regulation, while misinformation is not. The second challenge is determining who should be in control of regulations and their implementation; governments, independent commissions, or self-regulations by the social media and internet companies themselves could all play a role. Finally, there is the issue of what effective disinformation should look like, and what it should avoid.

The challenges are real, and daunting, but thoughtful efforts toward disinformation regulation have already begun. When we distill these early efforts down to their consistent themes, and view them through Tworek's historical lens, four standards for effective disinformation regulation stand out. First, is a regulatory Hippocratic oath: disinformation regulation should target the negative effects of disinformation while minimizing any additional harm caused by the regulation itself. Second, regulation should be proportional to the size of the harm caused by the disinformation and the economic realities of the companies potentially subject to regulations. Third, effective regulation must be nimble, and able to adapt to changes in technology and disinformation strategies more than previous communication regulations. Fourth, effective regulations should be determined by independent agencies or organizations that are guided by ongoing research in this field.

It is extremely difficult to effectively regulate online disinformation. However, understanding the complex sources of the regulatory challenges, and the historical patterns that have contributed to them, will help current and future efforts toward curbing the harms caused by online disinformation. The Eurasia Center was correct, there is no single fix, or set of fixes that will completely mitigate the dangers of strategic disinformation campaigns. However, the four standards identified in this chapter can help serve as a guide, as online disinformation and the regulatory efforts to stop it, continue into the future.

NOTES

1. Samantha Bradshaw and Philip N Howard, "Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation," Oxford Internet Institute, 2018, http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/07/ct2018.pdf.

2. The report entitled "Democratic Defense Against Disinformation," offers a very comprehensive list of potential actions that governments, civil-society, and private companies in the United States and Europe should take to mitigate the effects of malicious disinformation, like that spread by Russia during the 2016 residential election; Daniel Fried and Alina Polyakova, "Democratic Defense Against Disinformation," Atlantic Council – Eurasia Center, March 2018, www.atlanticcouncil.org/in-depth-research-reports/report/democratic-defense-against-disinformation/.
3. Nir Grinberg et al., "Fake news on Twitter during the 2016 U.S. presidential election," *Science*, 363, no. 6425 (2019): 374–378.
4. Yochai Benkler, Robert Faris, and Hal Roberts, *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics* (New York: Oxford University Press, 2018); Andrew Chadwick, *The Hybrid Media System: Politics and Power* (New York: Oxford University Press, 2013).
5. W. Lance Bennett and Steven Livingston, "The disinformation order: Disruptive communication and the decline of democratic institutions," *European Journal of Communication*, 33, no. 2 (2018): 122–139; Hossein Derakhshan and Claire Wardle, "Information Disorder: Definitions" (paper presented at the "Understanding and Addressing the Disinformation Ecosystem" Workshop, Philadelphia, December 15–16, 2017); Natalie Jomini Stroud, Emily Thorson, and Dannagal Young, "Making Sense of Information and Judging its Credibility" (paper presented at the Understanding and Addressing the Disinformation Ecosystem, Philadelphia, December 15–16, 2017); Don Fallis, "What is disinformation?," *Library Trends*, 63, no. 3 (2015): 401–426; M. Connor Sullivan, "Why librarians can't fight fake news," *Journal of Librarianship and Information Science*, 51, no. 4 (2019): 1146–1156; Leonie Haiden and Jente Althuis, "The Definitional Challenges of Fake News," King's Centre for Strategic Communications, Department of War Studies, King's College London, June 2018; Jente Althuis and Leonie Haiden, eds., *Fake News: A Roadmap* (Riga: The NATO Strategic Communications Centre of Excellence, 2018); Mark Verstraete, Derek E. Bambauer, and Jane R. Bambauer, "Identifying and Countering Fake News," SSRN Scholarly Paper, July 2017. See also the useful discussion and definitions in Benkler, Faris, and Roberts, *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*, 14.
6. Haiden and Althuis, "The Definitional Challenges of Fake News."
7. Claire Wardle, "Information Disorder: The Definitional Toolbox," *First Draft News*, July 6, 2018, https://firstdraftnews.org/infodisorder-definitional-toolbox/; Claire Wardle and Hossein Derakhshan, "Information Disorder: Toward an interdisciplinary framework for research and policy making," Council of Europe Report, 27 (2017).
8. One additional and distinct type of dangerous information has been labeled "malinformation," which is genuine or true information that includes private or revealing information, which is specifically disseminated to cause harm, andhas been the source of regulatory policy in many states in the United States

and nations around the world. Wardle, "Information Disorder: The Definitional Toolbox"; Derakhshan and Wardle, "Information Disorder: Definitions"; Daniel Funke and Daniela Flamini, "A Guide to Anti-misinformation Actions around the World," Poynter, updated April 9, 2019, www.poynter.org/ifcn/anti-misinformation-actions/.

9. Claire Wardle, "Fake news. It's complicated," *First Draft News*, 2017, https://medium.com/1st-draft/fake-news-its-complicated-d0f773766c79.
10. Derakhshan and Wardle, "Information Disorder: Definitions."
11. President Trump used the term fake news on Twitter 778 times during the 1,256 days he has been in office through June 28, 2020. This is an average of one mention every 1.61 days. What may be surprising is that as a candidate, Trump did not tweet about fake news once. His first mention of the term on Twitter was December 10, 2016, over a month after his electoral victory, and he started using the term regularly on Twitter just a few days before his inauguration. The tactic of dismissing critical news coverage as fake news was quickly embraced by leaders around the world, most notably by a number of strong-arm authoritarian leaders. All data taken from the Trump Twitter Archive, 2020, last accessed June 28, 2020, www.newsweek.com/fake-news-donald-trump-world-leaders-1165892; Tom O'Connor, "'Fake News!' Following Donald Trump, These Other World Leaders Have Blamed the Media for Troubles at Home," *Newsweek*, October 11, 2018, www.newsweek.com/fake-news-donald-trump-world-leaders-1165892; Sullivan, "Why librarians can't fight fake news."
12. High Level Expert Group on Fake News and Online Disinformation, "A Multi-dimensional Approach to Disinformation," European Commission, March 2018, 10–11, https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation
13. Samanth Subramanian, "Inside the Macedonian Fake-News Complex," *WIRED*, February 15, 2017, www.wired.com/2017/02/veles-macedonia-fake-news/.
14. Paul Mozur, "A Genocide Incited on Facebook, with Posts from Myanmar's Military," *New York Times*, October 15, 2018, www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html.
15. European Commission High Level Expert Group on Fake News and Online Disinformation, "A multi-dimensional approach to disinformation."
16. Newman Nic et al., "Reuters Institute Digital News Report 2018," Reuters Institute for the Study of Journalism, 2018; Richard Fletcher, "Misinformation and Disinformation Unpacked," Reuters Institute, 2018, www.digitalnewsreport.org/survey/2018/overview-key-findings-2018/
17. Jon Henley, "Global crackdown on fake news raises censorship concerns," *The Guardian*, April 24, 2018, www.theguardian.com/media/2018/apr/24/global-crackdown-on-fake-news-raises-censorship-concerns.
18. David M. J. Lazer et al., "The science of fake news," *Science*, 359, no. 6380 (2018): 1094–1096.
19. Eszter Hargittai, "An update on survey measures of web-oriented digital literacy," *Social Science Computer Review*, 27, no. 1 (February 2009): 130–137; David Buckingham, "Defining Digital Literacy: What Do Young People Need to Know About Digital Media?," in Colin Lankshear and

Michele Knobel, eds., *Digital Literacies: Concepts, Policies and Practices*, (New York: Peter Lang Publishing, 2008); David Bawden, "Functional Internet Literacy: Required Cognitive Skills with Implications for Instruction," in *Digital Literacies: Concepts, Policies and Practices*; Barbara R. Jones-Kavalier and Suzanne L. Flannigan, "Connecting the Digital Dots: Literacy of the 21st Century," *EDUCASE Quarterly*, 2006; Yoram Eshet-Alkalai, "Digital Literacy: A Conceptual Framework for Survival Skills in the Digital Era," *Journal of Educational Multimedia and Hypermedia*, 13, no. 1 (2004): 93–106; Melissa Tully, Emily K. Vraga, and Leticia Bode, "Designing and Testing News Literacy Messages for Social Media," *Mass Communication and Society*, 23, no.1 (2020): 22–46; M. Laeeq Khan and Ika Karlina Idris, "Recognise misinformation and verify before sharing: a reasoned action and information literacy perspective," *Behaviour & Information Technology*, 38, no. 12 (2019): 1194–1212; Emily K. Vraga and Leticia Bode, "I do not believe you: how providing a source corrects health misperceptions across social media platforms," *Information, Communication & Society*, 21, no. 10 (2017): 1337–1353; Emily K. Vraga and Leticia Bode, "Leveraging institutions, educators, and networks to correct misinformation: a commentary on Lewandosky, Ecker, and Cook," *Journal of Applied Research in Memory and Cognition*, 6, no. 4 (2017): 382–388; S. Mo Jang and Joon K. Kim, "Third person effects of fake news: Fake news regulation and media literacy interventions," *Computers in Human Behavior*, 80, no. C (2018): 295–302; Sullivan, "Why librarians can't fight fake news"; John N. Berry, "The misinformation age," *Library Journal*, 141, no. 14 (2016).

20. Funke and Flamini, "A guide to anti-misinformation actions around the world."
21. Ben Epstein, "The Stabilizing Window is Closing: How the History of Media Regulation Can Shape the Future of the Internet," Media, Technology, and Democracy in Historical Context Workshop, Brooklyn, NY, Social Science Research Council, May 16–17, 2019.
22. Pete Norman, "U.S. Unleashes Military to Fight Fake News, Disinformation," *Bloomberg*, August 31, 2019, www.bloomberg.com/news/articles/2019-08-31/u-s-unleashes-military-to-fight-fake-news-disinformation.
23. Irene Wu, "Who regulates phones, television, and the Internet? What makes a communications regulator independent and why it matters," *Perspectives on Politics*, 6, no. 4 (2008): 769–783.
24. Ben Epstein, *The Only Constant Is Change: Technology, Political Communication, and Innovation Over Time* (New York: Oxford University Press, 2018).
25. Declan Walsh and Nada Rashwan, "'We're at War': A Covert Social Media Campaign Boots Military Rulers," *New York Times*, September 6, 2019, www.nytimes.com/2019/09/06/world/middleeast/sudan-social-media.html?action=click&module=Top%20Stories&pgtype=Homepage.
26. Tim Wu, "Cyberspace sovereignty – The Internet and the international system," *Harvard Journal of Law & Technology*, 10, no. 4 (1996) 647–666; Stephan Wilske and Teresa Schiller, "International jurisdiction in cyberspace:

Which states may regulate the Internet," *Federal Communications Law Journal*, 50, no. 1 (1997): 117–178; Jack L. Goldsmith and Tim Wu, *Who Controls the Internet?: Illusions of a Borderless World* (New York: Oxford University Press, 2006); Jack Goldsmith, "Regulation of the Internet: Three persistent fallacies," *Chicago-Kent Law Review*, 73, no. 4 (1997): 1119–1131; Robert J. Domanski, *Who Governs the Internet?: A Political Architecture* (London: Lexington Books, 2015).

27. European Commission, "Tackling Online Disinformation," 2018, https://ec.europa.eu/digital-single-market/en/fake-news-disinformation; European Commission High Level Expert Group on Fake News and Online Disinformation, "A multi-dimensional approach to disinformation."
28. Nic et al., "Reuters Institute Digital News Report 2018."
29. Fletcher, "Misinformation and Disinformation Unpacked"; Nic et al., "Reuters Institute Digital News Report 2018."
30. John F. McGuire, "When Speech Is Heard around the World: Internet Content Regulation in the United States and Germany," *New York University Law Review*, 74 (1999) 750–792; Yana Breindl and Bjoern Kuellmer, "Internet content regulation in France and Germany: Regulatory paths, actor constellations, and policies," *Journal of Information Technology & Politics*, 10, no. 4 (2013): 369–388.
31. Tim Hwang, "Dealing with Disinformation: Evaluating the Case for CDA 230 Amendment," SSRN Scholarly Paper, December 17, 2017, http://dx.doi.org/10.2139/ssrn.3089442.
32. Kjerstin Thorson and Chris Wells, "Curated flows: A framework for mapping media exposure in the digital age," *Communication Theory*, 26, no. 3 (2015): 1–20; Chadwick, *The Hybrid Media System: Politics and Power*.
33. Casey Newton, "How Extremism Came to Thrive on YouTube," *The Verge*, April 3, 2019, www.theverge.com/interface/2019/4/3/18293293/youtube-extremism-criticism-bloomberg.
34. Ibid.
35. Alexander Pirang, "Germany's Half-Baked Approach to Fighting Disinformation," Council on Foreign Relations, April 12, 2018, www.gppi.net/2018/04/12/germany-wants-to-fight-disinformation-but-its-approach-is-half-baked. For more on Cambridge Analytica and why the company was selling a data version of snake oil, see Dave Karpf, "A World Without Wizards: On Facebook and Cambridge Analytica," *Civicist*, April 24, 2018, https://civichall.org/civicist/world-without-wizards-facebook-cambridge-analytica/; Dave Karpf, "Will the Real Psychometric Targeters Please Stand Up: A Skeptic's Take on Trump's Purported Big Data Juggernaut, Cambridge Analytica," *Civicist*, February 1, 2017, https://civichall.org/civicist/will-the-real-psychometric-targeters-please-stand-up/.
36. Tim Wu, *The Curse of Bigness: Antitrust in the New Gilded Age* (New York: Columbia Global Reports, 2018).

37. Chris Hughes, "I Co-Founded Facebook. It's Time to Break It Up," *New York Times*, May 9, 2019, www.nytimes.com/video/opinion/100000006480848/chris-hughes-facebook-zuckerberg.html?searchResultPosition=2.
38. Taylor Telford and Tony Romm, "New York, 7 Other States and D.C. Launch Antitrust investigation of Facebook," *Washington Post*, September 6, 2019, https://beta.washingtonpost.com/business/2019/09/06/new-york-announces-antitrust-investigation-into-facebook-kicking-off-bipartisan-effort/.
39. Kurt Wagner, "Facebook Meets with FBI to Discuss 2020 Election Security," *Bloomberg*, September 4, 2019, www.bloomberg.com/news/articles/2019-09-04/facebook-meets-with-fbi-to-discuss-2020-election-security.
40. David Kirkpatrick, *The Facebook Effect: The Inside Story of the Company That Is Connecting the World* (New York: Simon and Schuster, 2011); Kate Klonick, "The new governors: the people, rules, and processes governing online speech," *Harvard Law Review*, 131 (2017): 1598–1670.
41. Fletcher, "Misinformation and Disinformation Unpacked"; Nic et al., "Reuters Institute Digital News Report 2018."
42. Bertelsmann Foundation, *Self-Regulation of Internet Content* (Gutersloh, Germany: Bertelsmann Foundation,1999); Monroe Edwin Price and Stefaan G. Verhulst, *Self-Regulation and the Internet* (The Hague: Kluwer Law International BV, 2005); Milton Mueller, "ICANN and Internet governance: sorting through the debris of 'self-regulation,'" *Info, the Journal of Policy, Regulation and Strategy for Telecommunications Information and Media*, 1, no. 6 (1999): 497–520.
43. Bruno Lupion Goncalves, "Self-regulating internet platforms: Political and policy dynamics that shaped the EU Code of Practice on Disinformation" (Masters thesis, Hertie School of Governance, 2019).
44. Goncalves, "Self-regulating internet platforms: Political and policy dynamics that shaped the EU Code of Practice on Disinformation."
45. International Grand Committee on Big Data, Privacy, and Democracy, "Remarks to the International Grand Committee on Big Data, Privacy, and Democracy," 2019, www.cgai.ca/international_grand_committee_on_big_data_privacy_and_democracy.
46. Margaret O'Mara, "Letting the Internet Regulate Itself Was a Good Idea – in the 1990s," *New York Times*, July 5, 2019, www.nytimes.com/2019/07/05/opinion/tech-regulation-facebook.html?action=click&module=Opinion&pgtype=Homepage&login=smartlock&auth=login-smartlock.
47. Margaret O'Mara, *The Code: Silicon Valley and the Remaking of America* (New York: Penguin, 2019).
48. Peter Kafka, "The US Government Isn't Ready to Regulate the Internet. Today's Google Fine Shows Why," *Vox*, September 4, 2019, www.vox.com/recode/2019/9/4/20849143/youtube-google-ftc-kids-settlement-170-million-coppa-privacy-regulation; Tony Romm, "Facebook will have to pay a record-breaking fine for violating users' privacy. But the FTC wanted more," *Washington Post*, July 22, 2019, www.washingtonpost.com/technology/2019/07/22/facebook-vs-feds-inside-story-multi-billion-dollar-tech-giants-privacy-war-with-washington/?arc404=true.

49. Wardle and Derakhshan, "Information Disorder: Toward an interdisciplinary framework for research and policy making."
50. Commission on Truth Trust and Technology, "Tackling the Information Crisis: A Policy Framework for Media System Resilience," The London School of Economics and Political Science, 2018, www.lse.ac.uk/media-and-communications/assets/documents/research/T3-Report-Tackling-the-Information-Crisis-v6.pdf.
51. Brendan Nyhan and Jason Aaron Reifler, "Misinformation and Fact-checking: Research Findings from Social Science," New America Foundation, 2012, www.dartmouth.edu/~nyhan/Misinformation_and_Fact-checking.pdf; Joshua A. Tucker et al., "Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature," William & Flora Hewlett Foundation, March 2018, www.hewlett.org/wp-content/uploads/2018/03/Social-Media-Political-Polarization-and-Political-Disinformation-Literature-Review.pdf.
52. Emma Goodman, "The Online Harms White Paper: Its Approach to Disinformation, and the Challenges of Regulation," London School of Economics and Political Science, April 10, 2019, https://blogs.lse.ac.uk/medialse/2019/04/10/the-online-harms-white-paper-its-approach-to-disinformation-and-the-challenges-of-regulation/; Jeremy Wright and Sajid Javid, Online Harms White Paper, Department of State for Digital Culture, Media and Sport and Home Department, London, 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf.
53. Alex Hern, "Online harms white paper: could regulation kill innovation?," *The Guardian*, April 4, 2019, www.theguardian.com/technology/2019/apr/04/online-harms-white-paper-regulation-without-killing-innovation; Henley, "Global Crackdown on Fake News Raises Censorship Concerns."
54. Goodman, "The Online Harms White Paper: Its Approach to Disinformation, and the Challenges of Regulation."
55. Goodman, "The Online Harms White Paper: Its Approach to Disinformation, and the Challenges of Regulation"; Newton, "How Extremism Came to Thrive on YouTube."
56. "The EU General Data Privacy Regulation (GDPR) is the Most Important Change in Data Privacy Regulation in 20 Years," EUGDPR, 2018, https://eugdpr.org/; "Data Protection," European Union website, 2019, https://ec.europa.eu/info/law/law-topic/data-protection_en.
57. Fried and Polyakova, "Democratic Defense against Disinformation."