Article

Protecting Democracy from Disinformation: Normative Threats and Policy Responses

The International Journal of Press/Politics
2020, Vol. 25(3) 517–537

DOI: 10.1177/1940161220918740
journals.sagepub.com/home/hij
SAGE

Chris Tenove[1]

Abstract

Following public revelations of interference in the United States 2016 election, there has been widespread concern that online disinformation poses a serious threat to democracy. Governments have responded with a wide range of policies. However, there is little clarity in elite policy debates or academic literature about what it actually means for disinformation to endanger democracy, and how different policies might protect it. This article proposes that policies to address disinformation seek to defend three important normative goods of democratic systems: self-determination, accountable representation, and public deliberation. Policy responses to protect these goods tend to fall in three corresponding governance sectors: self-determination is the focus of international and national security policies; accountable representation is addressed through electoral regulation; and threats to the quality of public debate and deliberation are countered by media regulation. The article also reveals some of the challenges and risks in these policy sectors, which can be seen in both innovative and failed policy designs.

Keywords

online disinformation, democracy, election campaign, media law, Internet, policy making

Introduction

Since the 2016 election in the United States, policymakers, experts, and citizens have expressed alarm that online disinformation may threaten democracy. Russian interference in the election was "an attack on democracy itself," U.S. Senator Chuck Schumer

[1]The University of British Columbia, Vancouver, BC, Canada

Corresponding Author:
Chris Tenove, Department of Political Science, The University of British Columbia, C425 - 1866 Main Mall, Vancouver, Canada BC V6T 1Z1.
Email: cjtenove@mail.ubc.ca

(2019) told Congress (p. S2776). In the year following the U.S. 2016 election, at least seventeen countries had elections marred by disinformation, "damaging citizens' ability to choose their leaders based on factual news and authentic debate" (Freedom House 2017: 1). Social media companies are frequently seen as part of the problem: At Facebook's annual shareholder meeting in 2018, a plane flew overhead with a banner reading "YOU BROKE DEMOCRACY" (Osnos 2018).

Public opinion polls in many countries show that citizens fear that democracy is at risk. A survey in Europe found 83 percent of people believe democracy is threatened by fake news (European Commission 2018b); in Taiwan, 67.5 percent of people fear disinformation could cause "great harm" to the country's democracy (Taiwan Foundation for Democracy 2019); and in the United States, 68 percent of Americans identify "made-up news" as a significant threat to trust in government and a greater problem than terrorism, racism, or climate change (Stocking 2019).[1]

In response to these concerns, governments have proposed or adopted a wide range of policies. "If we do not regulate the Internet," warned French President Emmanuel Macron (2018), "there is the risk that the foundations of democracy will be shaken." Policy responses have ranged from offensive cyber-operations targeting disinformation actors to new regulations for social media platforms.[2] However, there is little clarity in elite policy debates or academic literature about what it actually means for disinformation to threaten democracy, and how different policies might protect democracy—or jeopardize it. To help clarify these debates, this article makes two contributions, both of which draw on an original survey of policy responses to disinformation by ten democratic states and the European Union (EU).

First, building on recent systemic frameworks in democratic theory, I identify three normative goods of democratic systems that policymakers have explicitly or implicitly claimed to be threatened by disinformation. These are the *self-determination* of polities by their own citizens; *accountable representation* through fair elections; and *public deliberation promoting opinion and will formation*. While these goods are interrelated, each highlights a different aspect of democratic political systems that can be harmed by disinformation, requiring different policy responses.

Second, I argue that threats to self-determination are primarily addressed through security policies at international and domestic levels; threats to democratic representation are principally addressed through new electoral regulations; and threats to deliberation are primarily addressed by media regulation. While communication scholars tend to focus on media regulation, most governments have enacted or proposed regulations in all three policy sectors, and policies in all three sectors have implications for news organizations as well as social media companies. Comparative policy analysis reveals some of the challenges of policy making in these areas, primarily due to regulatory capture, as well as examples of innovative and problematic policy designs.

I conclude by identifying key implications of this analysis for developing and evaluating policies to address disinformation.

Analyzing Policy Responses to Disinformation

In current policy-making documents and debates, disinformation usually refers to intentionally false or deceptive communication tactics that actors use to advance their political or economic aims. In a highly influential report, Wardle and Derakhshan (2017) contrast "disinformation," referring to *intentionally* false or deceptive communication, with "misinformation," which refers to communication that may contain false claims but is not intended to cause harm (such as satire or accidental errors). The term "disinformation" has also gained traction because it has long been used to analyze Russian information operations. Indeed, some policy responses by western governments to online disinformation have been grafted onto preexisting approaches to address strategic communication operations by Russia.

Some policymakers use cognate terms for disinformation, such as "information operations" and "information manipulation" (see, for instance, Facebook 2017; National Assembly 2018; NATO StratCom 2016). The term "disinformation" is increasingly seen as preferable to "fake news." As the European Commission's High Level Expert Group on Fake News and Online Disinformation (2018) argued, "fake news" does not aptly describe the many forms of misleading communication online, which go beyond false news stories to include manipulated images and videos, blends of fact and falsehood, and the deceptive use of automated or fake accounts (pp. 10–11). Furthermore, "fake news" has

> been appropriated by some politicians and their supporters, who use the term to dismiss coverage that they find disagreeable, and has thus become a weapon with which powerful actors can interfere in circulation of information and attack and undermine independent news media. (High Level Expert Group on Fake News and Online Disinformation 2018: 10; see also Digital, Culture, Media and Sport Committee 2018)

A powerful early narrative about disinformation in the 2016 U.S. election held that *foreign* actors played the leading role in undermining electoral integrity through the dissemination of false messages on social media platforms. However, subsequent analysis has shown that *domestic* political candidates, journalists, and citizens played major roles in promoting disinformation, and often did so to advance partisan interests (Benkler et al. 2018; Watts and Rothschild 2017). For this and other reasons, policy making to address disinformation has increasingly been politicized. It is clear that policy responses to disinformation—including decisions by some policymakers not to address the issue—may advantage or disadvantage different political factions. There are also serious concerns about the impact of disinformation policies on freedom of expression, a concern magnified by repressive states using such laws to attack journalists and political opponents. It is therefore important to bring rigorous normative analysis to sweeping claims about how disinformation or disinformation policies affect democracy.

Methodology: Democratic Theory and Policy Analysis

Greater conceptual clarity regarding the democratic threats posed by disinformation has two benefits. The first is to improve empirical analysis by specifying the democratic processes, institutions, or outcomes at risk. Empirical studies of the impact of disinformation on democracy frequently use different definitions of disinformation (as an independent variable) and different dependent variables, such as impacts on individual voter preference formation, communicative flows in information systems, electoral integrity, election outcomes, or trust in the media and other political institutions (see, for instance, Allcott and Gentzkow 2017; Benkler et al. 2018; Guess et al. 2018). This can be seen in the observation by Karpf (2017) that researchers can argue both that the relatively small ad buys by Russia-backed actors likely did not influence public opinion enough to swing the 2016 U.S. election, *and* that these violations of electoral law were a major attack on democratic processes. Different forms and impacts of disinformation are worth studying, but researchers should clearly define the variables they focus on.

Second, different understandings of the democratic threat posed by disinformation can be used to design and justify quite different policies. Normative claims and assumptions are central to policy making (Goodin et al. 2006), and journalism and media scholars have been encouraged to engage more substantively with normative theory, and democratic theory in particular (Christians et al. 2010; Karppinen 2013).

This article therefore uses democratic theory to identify the core normative goods that are explicitly or implicitly identified in responses to disinformation. I do so by analyzing policy-making documents and debates of the EU and ten democratic states: Australia, Canada, Denmark, France, Germany, Italy, Sweden, Taiwan, the United Kingdom, and the United States. Cases were selected to include countries with different media systems, drawing on classifications proposed by Hallin and Mancini (2004) and by Brüggemann et al. (2014). Taiwan is included as a nonwestern democracy that faces major disinformation threats, and the EU as a prominent policy actor with significant influence on European state policies. Case countries were selected for variation in media system in the expectation that this would yield more variation in policy responses to analyze, as different media system types feature different forms of government regulation. This article does not attempt to argue that particular media system types tend toward particular disinformation responses, although that is a hypothesis worth exploring.

Data regarding the normative propositions, organizational forms, and legal bases of policies are derived from more than 100 sources including original policy documents, government studies, major academic and think-tank reports, and news articles (primarily in English or French, some using translation software). As per the methodology of Kreiss et al. (2018), analysis proceeded by toggling between identifying emergent categories in the data and engaging with concepts from democratic theory and media studies. This analysis differs from proposing a freestanding normative framework, arrived at deductively from existing normative theory, and it also differs from inductively deriving normative claims through discourse analysis. Instead my approach is

abductive (Feilzer 2010), in that I identified both democratic goods under threat and key policy sectors involved by alternating between the analysis of policy documents and interpretation using alternate theoretical concepts. It is thus a form of "non-ideal" normative analysis, which operates "between abstract ideal models and mere empirical descriptivism, [and] which can function as a conceptual resource for evaluating, identifying, and pushing up against different ways in which actual, existing institutions, policies, and circumstances" can promote valued aims such as democratic communication (Karppinen 2019: 73).

This article's normative analysis draws on systemic approaches in democratic theory (e.g., Habermas 1996; Mansbridge et al. 2012; Warren 2017). Systemic approaches articulate key normative goods that a political system must promote for it be democratic, but do not dictate which good warrants primacy. This article generally employs the framework of Warren (2017), who proposes that a political system must do three things to advance the fundamental democratic commitment that *the people should rule themselves*. The three functions are empowering the inclusion of individual members in decisions that affect them (such as through rights to vote in elections, organize for causes, or contribute to public debates about political issues), forming collective agendas and wills (such as through communication that enables people to see how their individual preferences relate to collective judgments), and making collective decisions (such as through binding elections). These basic functions of democratic systems may be promoted by different bundles of institutions and practices, which interact in complex ways. For instance, voting enables citizens to select representatives, hold them to account for their performance, and empower them to make decisions on behalf of the collective—which together I refer to as the democratic good of "accountable representation."

This analysis differs somewhat from two common approaches in political communication research. One approach applies a particular "model" of democracy, such as deliberative or participatory democracy (for a survey, see Karppinen 2013). Each "model" emphasizes a singular constellation of institutions, practices, and normative aims. However, actual democracies pursue multiple normative aims through multiple institutions and practices. Another common approach is to focus on citizens' roles as both media consumers and democratic participants, such as "informed" or "monitorial" citizens (Schudson 1998). Such analysis is useful for formulating regulative ideals for institutions and citizens, and evaluating their achievement in practice (see, for instance, Ytre-Arne and Moe 2018). However, it neglects key democratic activities beyond those of average citizens, such as the work of electoral management bodies or national security agencies.

Using concepts from systemic theories of democracy to interpret policy-making documents and debates, I identify three key normative goods at stake. These are *self-determination*, *accountable representation*, and *deliberative processes of opinion and will formation*. Each of the following sections clarifies one of these democratic goods and the risks it faces from online disinformation, examines policy responses that were arguably designed to address those risks, and identifies challenges posed by such policies.[3]

Protecting Self-Determination: International and National Security Policies

The head of the United Kingdom's M16 intelligence agency stated in 2016 that online propaganda and cyber-attacks "represent a fundamental threat to our sovereignty. They should be a concern to all those who share democratic values" (MacAskill 2016). Many governments and policymakers have echoed this concern that disinformation threatens democracy because it undermines national security and—in the international context—sovereignty. This section argues that the normative good of "self-determination" clarifies this understanding of threats to security and sovereignty as threats to democracy. It then examines recent international and national security policies addressing disinformation, and highlights democratic risks of treating disinformation as a security threat.

Disinformation as a Threat to Self-Determination

From ancient Athens to the U.S. constitution to twentieth-century de-colonization struggles, political leaders and thinkers have argued that for a people to rule themselves they must be free from external domination, as well as from domination by domestic rulers or elites (Gould 2006; Habermas 1996; Young 2000). This conviction is frequently referred to as self-determination. Disinformation is an attack on democratic self-determination if it undermines or seeks to undermine the ability of a democratic people to enact the collective rules that they have given themselves, or if it compromises the selective empowerments that enable citizens to contribute to giving themselves rules (such as a right to vote in fair elections, or to freely contribute to public discourse on political issues).[4] Concerns about self-determination thus focus on how disinformation—particularly from foreign actors—can inappropriately include or exclude people from democratic processes, including processes like elections and public deliberation which will be discussed later.

Does that mean that any foreign influence is a threat to self-determination? Many contemporary democratic theorists disagree. They argue that noncitizens or foreigners *should* influence the democratic processes of states because, in a globalized world, the actions of one state can have significant consequences for people in other states (see, for instance, Gould 2006; Young 2000). However, there can certainly be justifiable limits to influence by foreign actors, particularly if they are needed to protect the selective empowerments conferred on citizens. As Gould (2006) argues, even if present day global interdependence means that "sovereignty in a strong sense is no longer applicable," the democratic good of self-determination limits the justifiable forms of foreign involvement (p. 51).

International Security Policies to Address Disinformation

International law does not provide clear guidelines for states to respond to foreign disinformation campaigns, even when they occur during elections (Hollis 2018; Ohlin

2017). Cybersecurity breaches that disrupt critical state activities *could* be seen as violations of state sovereignty that justify coercive state retaliation, on the basis of self-defense under Article 51 of the United Nations Charter. However, while cyber-operations that target physical infrastructure or data systems may clearly harm state functions, it is much more difficult to make that argument regarding disinformation, as it affects people's beliefs, emotions, and cognitive processes. International law, observes Hollis (2018), is a poor instrument to regulate "activities primarily defined by their connection to the cognitive dimension. There is so much uncertainty about evidence, causation, and motivations, that any new law is likely to prove ineffective from the outset" (p. 44). Finally, customary international law does not appear to prohibit information operations to influence another state's elections, as states have regularly done so without prompting coercive retaliation.

While governments have not proposed new treaties to address foreign disinformation, they have created new operational policies that treat disinformation as a security threat. The North Atlantic Treaty Organization (NATO) alliance and its institutions have identified disinformation as a key aspect of "hybrid warfare," and increasingly coordinate their military and intelligence capabilities to address it (NATO StratCom 2016). The G7 created the "Charlevoix Commitment on Defending Democracy from Foreign Threats," which includes a Rapid Response Mechanism to coordinate states' intelligence and policing agencies to better identify and counter disinformation and election interference (Government of Canada 2019). The most active international cooperation on foreign disinformation occurs within the EU (European Commission 2018b). Initiatives focus on security sector coordination, as well as the electoral and media regulations discussed later.

National Security Policy Responses

Governments have turned to their national security sectors to address online disinformation by foreign or domestic actors. National security actions take a variety of forms, from criminal law enforcement to intelligence gathering to offensive cyber-operations.

As an illustrative case, Canada created an intergovernmental task force to coordinate intelligence agencies, federal police, and the foreign affairs department to address disinformation (for an overview of Canadian disinformation policies, see Tenove and Tworek 2019). It also created a nonpartisan panel to receive intelligence briefings during election campaigns and decide whether to alert elected officials or the general public about electoral interference. The panel addresses fears that—in the midst of an election campaign—neither security agencies themselves nor the governing party can publicize interference without concerns that they are doing so to illegitimately bias the election outcome.

Like Canada, Nordic countries developed comprehensive national security plans to address foreign disinformation (Cederberg 2018; Government of Denmark 2018). These include cybersecurity and intelligence components, but they also emphasize media literacy and public resilience. For instance, every Swedish household received a national emergency brochure that included information about disinformation campaigns (Jeangène

Vilmer et al. 2018: 120), and the Swedish defense department frequently shares information with news media, including by regular Media Preparedness Councils (Cederberg 2018). Nordic governments have also emphasized strategic communication by the security sector (Pamment et al. 2018), a tactic that the EU has primarily assigned to the East StratCom Task Force.

Finally, military and intelligence agencies have contemplated or used offensive cyber-operations to address online disinformation, such as hack-backs and counterinformation operations. For instance, to address potential interference in its 2018 midterm elections, the U.S. military temporarily blocked Internet access to the Russian firm responsible for disinformation campaigns in the 2016 election (Nakashima 2019).

Challenges to Security Responses to Disinformation

Treating disinformation as a national security threat often makes sense. Disinformation tactics could undermine a people's capacity to enact its decisions via their democratic government (such as by fabricating orders from public officials), or compromise a people's ability to contribute to rule making (such as by circulating news of a natural disaster on a voting day). Furthermore, foreign governments can mobilize enormous resources, and so governments may similarly need to martial their capacities to counteract them. Indeed, only state security agencies have the combination of signals intelligence and human intelligence needed to discover coordinated and covert disinformation campaigns.

However, security agencies have fraught relationships with democracy. Their interference in domestic political affairs can lead to excessive influence in democratic processes by the governing party or by security agencies themselves. A national security logic may unduly interpret false or partly false communications as security risks, rather than as opportunities for correction and debate. As Farrell and Schneier (2018) observe, national security frameworks tend to see opportunities for contentious communication as vulnerabilities rather than virtues: "This means that the national security approach has enormous difficulties in assessing the appropriate trade-offs that are needed to guarantee a well-functioning democracy" (p. 5).

Moreover, a national security–focused approach can shift policy making and especially policy enforcement to government agencies that tend to be under weak democratic control. The national security agencies of many countries "are typically subject to limited oversight and accountability, and are historically separated from the citizenry by secrecy, hierarchy, and virtually unchecked executive power" (Deibert 2018: 413). This issue can be seen in struggles by journalism organizations to report on security agencies, even in countries with strong protections for a free press (Lidberg and Muller 2018).

The repressive use of national security laws against disinformation by authoritarian countries is well-documented (Henley 2018), but concerns have also been raised about security policies in democracies. One example is Taiwan's response to potential Chinese disinformation operations. In the lead-up to the 2020 election, Taiwan passed the Anti-Infiltration Act that targets foreign interference through

disinformation, lobbying, and other means (Aspinwall 2020). The government also pressured its National Communications Commission to crack down on domestic news organizations for false and biased reporting that may advance China's influence. The former head of the Commission, who allegedly resigned because she did not agree with this crackdown, warned, "The government says disinformation is the enemy of an open and democratic society . . . But we don't want to lose that open society by fighting against it" (Aspinwall 2020).

Protecting Accountability and Representation: Electoral Regulation

Governments routinely characterize disinformation as a threat to electoral integrity and thus to democracy. For instance, the European Commission (2018a) declared that elections "have proven to be periods which are particularly prone to targeted disinformation. These attacks affect the integrity and fairness of the electoral process and citizens' trust in elected representatives and as such they challenge democracy itself" (p. 1). This section clarifies the democratic goods at stake in election interference, identifies recent policies, and highlights some risks and limitations of these policy responses.

Disinformation as a Threat to Accountable and Representative Government

Elections are not themselves a normative good; rather, they are core processes for achieving the democratic good of accountable representation. Elections that do not advance this are empty procedures, as seen in elections conducted by authoritarian regimes.

Democratic elections enable citizens to select their political representatives, create representative bodies that can engage in deliberation and bargaining, and regularly hold to account their representatives and elected government for past conduct (Manin 1997; Przeworski 1999). For elections to promote these goods, there must be choice and fair competition among potential representatives, all citizens must have an opportunity to select a representative, and communicative forums must exist so citizens can learn about potential representatives and engage in macro-level "conversations" with them (Young 2000: 121–28).

Online disinformation campaigns can target important elements of elections that advance democratic representation and accountability. These could include false claims about where, when, and how to vote, such as those spread by Russia-backed actors to certain demographic groups in the U.S. 2016 election (DiResta et al. 2018). Disinformation campaigns can also damage fair competition among candidates and parties, such as the false stories targeting presidential candidate Macron in the 2017 French election (Jeangène Vilmer et al. 2018: 106–110). In addition, foreign and domestic actors can violate prohibitions or limits on campaign spending, including

through the use of false accounts to purchase and spread information on social media platforms (Chaykowski 2017). These and other efforts may undermine self-determination as well as election integrity, especially if foreign actors damage the empowerments and processes for members of a polity to contribute to ruling themselves.

Electoral Regulation to Address Disinformation

Disinformation campaigns during elections have revealed inadequacies in electoral regulation, particularly regarding activities on social media platforms. In a comment that could be applied to many countries, a U.K. parliamentary committee declared, "Electoral law in this country is not fit for purpose for the digital age, and needs to be amended to reflect new technologies" (Digital, Culture, Media and Sport Committee 2018: 15). Since 2016, many governments have proposed or adopted policies to respond to those inadequacies.

The most straightforward use of disinformation to undermine electoral integrity is to spread false information about voting processes, candidates, or election issues. While some governments already had laws against certain false communications in the context of election campaigns, these were not designed for the situation where actors can spread misleading claims widely, quickly, and surreptitiously via social media platforms.

France has introduced some of the most forceful electoral policies to counter false information online in elections. Preexisting laws address false and fabricated communication by targeting their creator or propagator; they were ill-suited to situations where the originators and disseminators of messages may remain unknown (Smith 2019). The new legislation enables judges to receive complaints about false information online and, if it violates the law, to order its immediate removal by social media companies or Internet service providers (National Assembly 2018). In addition, the French broadcasting agency was given the authority to suspend or terminate the activity of broadcasters under the influence of foreign states, if they spread false information likely to undermine electoral integrity. The legislation also requires social media platforms to disclose payments made to promote messages during elections, and to create mechanisms for users to alert the companies and government authorities about false information related to the election.

In addition to spreading false information, disinformation actors have violated the letter or spirit of electoral finance regulations (e.g., Chaykowski 2017; Karpf 2017). Such laws apply to how resources are acquired and deployed in elections, often to amplify electoral messaging. Since 2016, governments have clarified and tightened laws, particularly with respect to foreign actors. For instance, the Australian government passed both the *Electoral Funding and Disclosure Reform Act* and the *Foreign Influence Transparency Scheme Act*, largely due to fears of Chinese influence operations (Douek 2018).

Governments have also adopted policies to improve the transparency of political advertising, primarily through the creation of publicly accessible ad archives. Improving transparency is expected to increase the likelihood that citizens, watchdog

organizations, and regulators can catch false or illegal advertising, even when they are micro-targeted toward particular segments of the electorate. Canada and France introduced laws that require social media companies to create ad repositories; the EU's Code of Practice on Disinformation commits signatories (which include all major social media companies) to create ad repositories and parliamentary committees in the United Kingdom and the Netherlands have proposed regulations to require ad archives (Leerssen et al. 2019). A similar proposal in the United States, the Honest Ads Act, has stalled despite bipartisan support. Facebook and other social media companies have responded by creating political ad archives, including in the U.S. More recently, in the face of mounting concerns about the accuracy and targeting of political ads, Twitter announced it will not allow explicit political advertising, Google will limit the targeting of political ads and submit certain advertising claims to fact checking, and Facebook will continue to allow targeting and will shield political ads from its fact checking (Ingram 2020).

Challenges to Electoral Regulations to Address Disinformation

Even before the rise of social media platforms, electoral regulations in many countries struggled to address false information in broadcasts, publications, and advertisements, and failed to enforce electoral spending limits and transparency measures. These challenges increase when attribution is difficult, as it frequently is for disinformation efforts on social media platforms. Attribution is necessary for enforcement and thus for deterrence; it is also necessary for policies that seek to apply different rules to foreign and domestic entities. For this reason, electoral regulations are often combined with increased national security efforts that attempt to identify foreign activities, as has been done by governments including Australia, Canada, Taiwan, and the EU.

It is relatively uncontroversial for governments to prohibit messages that might straightforwardly lead to disenfranchisement, such as false claims about how to vote. Governments face greater challenges when trying to regulate the content of claims about candidates and issues. Such regulations provoke concerns about freedom of expression, and also about opportunities for captured government agencies to unduly influence messaging during election campaigns.

While France's regulation of false claims in elections appears to adhere to rule of law provisions to protect free expression and avoid capture by the government and governing party (Smith 2019), other countries' policies are more problematic. For instance, in 2018, Italy enacted the "Operating Protocol for the Fight Against the Diffusion of Fake News through the Web on the Occasion of the Election Campaign for the 2018 Political Elections," which gave the Postal Police the authority to determine if online claims are false or biased and recommend judicial action (Verza 2018). Giving the police a discretionary role to assess and act on content was strongly criticized by experts (Verza 2018), including the United Nations special rapporteur for the protection of freedom of expression (Kaye 2018a), and by journalism organizations that saw the law as a potential threat to a free press (Funke 2018).

Protecting Deliberation: Media Regulation

Many policy proposals emphasize the threat that disinformation poses to the quality of public discourse and debate. These values are best captured by analyses of democracies as deliberative systems. As the LSE Commission on Truth, Trust and Technology (2018) argues, democracies "must ensure that the infrastructure of deliberation—and that means the news media and digital information systems—are up to the task of generating informed dialogue" (p. 12). Rather than targeting disinformation actors themselves, as do most national security and election policies, media policies seek to reduce the vulnerabilities of media systems that those actors exploit.

Disinformation as a Threat to Democratic Deliberation

Theories of deliberative democracy propose that communicative exchanges among citizens are necessary to achieve well-informed and legitimate public decision making (Habermas 1996; Young 2000). These communicative exchanges promote what theorists sometimes call "opinion formation" (the development of reasonably informed individual preferences) and collective "will formation" (coming to understand reasons for collective judgments). Democratic theorists have increasingly developed systemic approaches to understand how the normative goods of deliberation can be achieved in the real world. Systemic approaches do not require that citizens and public officials frequently meet stringent requirements of deliberation. Instead, the payoffs of deliberation can be achieved through a division of deliberative labor among different forums and institutions, producing both particular instances of deliberation and an overall deliberative quality. A well-functioning system will have sites of discourse that are linked to decision making (like parliaments and courtrooms), and these should be informed by and accountable to discourse among citizens in the "wild" public sphere (Habermas 1996; see also Dryzek 2009; Mansbridge et al. 2012). Deliberation in a political system, achieved through interactions between interconnected forums, should promote three normative goods: epistemic quality, moral respect, and democratic inclusion (Mansbridge et al. 2012). Disinformation campaigns may threaten all three (Tenove and McKay 2019).

Disinformation campaigns may cause systemic harm to epistemic quality if they promote false claims at a large scale, or if they discourage citizens from engaging with high-quality sources of information. For instance, Russia-backed actors promoted pseudoscience conspiracies about vaccination, climate change, and other issues online, while also attacking expert institutions that make high-quality information claims (DiResta et al. 2018). Another tactic is to encourage a sense of helplessness about finding accurate or authentic claims, an objective of the Russian "firehose of falsehood" propaganda strategy (Paul and Matthews 2016).

Online disinformation campaigns frequently aim to corrode moral respect toward social groups, including those that already face obstacles to full political participation (DiResta et al. 2018; Spaulding et al. 2018). In addition to targeting social groups, online disinformation includes false claims, conspiracy theories, chauvinistic

language, and imagery that stokes moral revulsion toward electoral candidates and public officials.

Finally, disinformation tactics offer new means to reduce opportunities for people to be included in discourse on issues that significantly affect them. For instance, foreign or domestic actors can use bots, fake accounts, promoted posts, and other techniques to flood communicative forums, and drown out opportunities for individuals to contribute or encounter diverse views (DiResta et al. 2018; Woolley and Guilbeault 2018). (This is not to deny that digital media can expand some people's opportunities to engage in public discussions of political issues, including perspectives that were marginalized in previous media systems).

In sum, disinformation may undermine a deliberative system not only by increasing the quantity of false claims in circulation but also by decreasing people's interest and opportunity to engage in public discussions on terms of reason giving, respect, and inclusivity.

Social Media Regulations in Response to Disinformation

All democracies regulate mass media organizations to enhance democratic debate (Puppis 2014). Since 2016, governments have introduced new media policies in an effort to address disinformation. These have focused on social media, both because social media platforms were major vectors for disinformation and because they largely existed in regulatory gaps.

The global foundation of social media regulation is Section 230 of the U.S. 1996 Communications Decency Act (CDA). This provision enables social media companies to moderate the content that users share on their platforms without being legally responsible for that content (with some exceptions). Because social media companies were based in the United States, this regime was the de facto regulatory approach in most states prior to 2016. Indeed, the fact that social media regulation until recently has largely been done by the United States is arguably a violation of self-determination, as other democratic polities did not make and enforce their own rules over political speech.

Since then, the most prominent regulation of social media companies has been pursued by Germany, with its 2017 "NetzDG" law. The law requires large social media platforms to take swift action on content that likely violates one of Germany's preexisting statutes on illegal communication, or face a fine of up to fifty million Euros (Tworek and Leerssen 2019). NetzDG does not explicitly address disinformation but it does apply to defamation, propaganda advanced by banned organizations, and false claims that amount to hate speech, such as Holocaust denial. Furthermore, as attacks on moral respect may also undermine deliberation, NetzDG's prohibition on hate speech may protect the deliberative system. While there are concerns that the law incentivizes platforms to engage in large-scale, preemptive takedowns of legitimate speech, there is little evidence that this is occurring, although more research is necessary (Tworek and Leerssen 2019).

The EU has explicitly targeted disinformation using a coregulatory media approach. The European Commission encouraged key stakeholders to develop a Code of Practice

on Disinformation, which all major social media companies have now signed. The code includes commitments to reduce fake accounts and bots, improve advertising transparency, and improve users' ability to identify untrustworthy and trustworthy sources of information (Multistakeholder Forum on Disinformation 2018). The approach is coregulatory rather than self-regulatory because the European Commission has insisted on and evaluates indicators to determine if social media companies are adhering to the code, and threatened stronger regulation if its expectations are not met. As an example of stronger enforcement of a code of conduct, the Australian Competition and Consumer Commission (2019) proposed that an independent government body should have the authority to investigate potential violations of a code of practice and impose fines.

The United Kingdom put forward a somewhat different approach in its *Online Harms White Paper* (United Kingdom Parliament 2019). The policy would empower a regulatory body to enforce expectations regarding individuals' exposure to harms through social media use. As commentators and free speech organizations have observed, this approach may be straightforward for addressing illegal communication (such as revenge pornography or encouragement of suicide), but vague claims about disinformation and its harms may result in a framework that violates rights to freedom of expression (Pomerantsev 2019).

In response to regulatory and public pressure, social media companies have significantly increased enforcement of their own terms of service, include prohibitions on spam, fake accounts, and deceptive advertisements. They have also worked with other groups to address the spread and impact of false claims. For instance, Facebook created partnerships with independent fact-checking organizations, and it reduces the discoverability of content that these organizations determine to be significantly false. There are extensive and valid criticisms of these efforts by Facebook, but they do seem to be having an effect. Engagements with fake news sites appears to have declined significantly on Facebook since 2016, although Facebook continues to play a major role in the diffusion of false or deceptive stories online (Allcott et al. 2019).

Challenges of Media Regulation to Address Disinformation

New social media regulations often seek to make companies enforce governments' expectations regarding users' problematic behavior (e.g., deceptive accounts, spam) and content (e.g., false claims, hate speech). Such measures can have a range of problematic outcomes. One is that they may be a means for governments to gain undue control over communication by citizens. This might limit people's abilities to expound and test positions, but could also be used to suppress criticism or gain unfair electoral advantages. A second concern is that regulations may incentivize social media companies to themselves become the judges and enforcers of speech regulations, without needing to adhere to rule of law standards such as opportunities for appeal. In both cases, social media regulation may threaten freedom of expression (ARTICLE 19 2018; Kaye 2018b).

A further risk is that policies could have unintended consequences, perhaps even increasing opportunities for disinformation. One policy proposal that may do so is the

"Ending Support for Internet Censorship Act," put forward by U.S. Senator Josh Hawley (Coaston 2019). The law would strip social media companies of their CDA Section 230 protections unless a government regulator declares them free of political bias. It would thus empower a government agency to be the key arbiter of political content. It would also incentivize platforms to refrain from moderating false, deceptive, or abusive content, out of fear that a government panel might interpret these actions as evincing bias. The proposed law, which is unlikely to be enacted, is a prime example of flawed social media regulation, potentially leading to both regulatory capture and increased incidence of disinformation.

Conclusion

Online disinformation has been a major focus of democratic governments following revelations of online interference in elections in the United States and elsewhere, generating numerous and diverse policy responses. This article has attempted to clarify the different ways in which disinformation might threaten democracy, focusing on the normative goods of self-determination, accountable representation, and public deliberation. By making concerns about threats to democracy more explicit, researchers and policymakers can more clearly specify and evaluate different types of harm. They can also make clearer recommendations regarding policies to address those harms. National security responses may be needed to address risks to key state activities such as the enforcement of election laws and also to ensure that illegitimate actors—especially foreign states—do not undermine full and fair participation in a democratic system. Electoral regulations may be needed to protect people's basic democratic empowerments, such as the right to vote, and to prevent efforts to compromise fair and transparent electoral competition. Media regulations should protect free expression in the wild public sphere while also cultivating media systems capable of supporting epistemically robust and morally respectful communication.

This article's analysis also highlights democratic risks posed by disinformation policies themselves. Here, too, conceptual clarity is necessary. Critics of disinformation policies often make vague assertions about their threat to freedom of expression. As Karppinen (2019) has observed, claims that regulations undermine freedom of expression are "often mobilized by those in power to block reforms and close down debate" (p. 72), and tend to ignore the many existing obstructions to the use of public speech, including "new forms of platform dominance and algorithmic censorship" (p. 68). This article has argued that the dangers of disinformation policies are not simply their restrictions on what individual people can say but also that they may unduly empower government agencies, governing political parties, or other entrenched interests to influence communication at crucial moments (including during election campaigns).

At the same time, a government's decision *not* to address disinformation may itself be an attempt to unduly empower some of these same entities. One striking feature of policy responses to disinformation since 2016 is the fact that the United States, the country that experienced the highest-profile campaigns of online election interference, has not enacted a significant regulatory response. While President Donald Trump has

not backed policies to address disinformation tactics that arguably contributed to his election, he has publicly supported measures to reduce alleged left-wing bias in social media content moderation (Vaidhyanathan 2019).

To navigate the challenges of policy responses to disinformation, policymakers can learn from each other's innovations and failures. The Italian government's 2018 "fake news" law, in which police units were authorized as fact checkers, is a good example of a defective policy. By contrast, the Canadian government's creation of a nonpartisan panel to make decisions about informing the public of disinformation during an election campaign is promising, as it takes this decision out of the hands of the governing party and does not leave it solely up to security agencies. The regular and extensive communication between Swedish intelligence agencies and journalists is another productive approach, as it leverages the insights of intelligence agencies but leaves public communication up to independent journalists.

This article's conceptual framework and policy survey do not lead to clear policy recommendations. Rather, they help clarify the normative goods at stake and the potential roles of different policy sectors to protect them. They may therefore sharpen questions for future research. How effective are different policy responses at addressing different types of democratic threat? How much do different media systems influence the means by which disinformation can be countered? When do different policy measures complement or undermine each other? And when might the poison of disinformation be less harmful for democracy than proposed policy cures?

Acknowledgments

Thank you to Jordan Buffie, Spencer McKay, Fenwick McKelvey, and Heidi Tworek for feedback and to Jordan Buffie for research assistance. The article also benefited from comments by participants in the Digital Threats to Democracy Threats to Democracy workshop, hosted by the Social Science Research Council in June, 2019.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: Support for this research was provided by the Social Sciences and Humanities Research Council of Canada.

ORCID iD

Chris Tenove https://orcid.org/0000-0002-4244-0878

Notes

1. As Nielsen and Graves (2017) rightly argue, surveys regarding people's concerns about fake news or disinformation should be further interrogated, as respondents may not be using researchers' definitions of these terms but may be articulating broader frustrations with news media, social media, or the quality of political discourse.

2. In addition to disinformation, policy-making responses have also identified democratic threats posed by issues including cybersecurity and the exploitation of people's private data. These issues are beyond the scope of this article, as they challenge democracy in somewhat different ways and require different policy responses.
3. Policy analysis in this article is illustrative rather than exhaustive. I highlight particular government policies to illustrate challenges in each policy sector. A full documentation of all policies of all government policies in all three sectors, or in-depth analysis of policy making by any particular government, is beyond the scope of this article.
4. For a complementary analysis of foreign disinformation as an attack on self-determination, see Ohlin (2017).

References

Allcott, H., and M. Gentzkow. 2017. "Social Media and Fake News in the 2016 Election." *Journal of Economic Perspectives* 31 (2): 211–36.

Allcott, H., M. Gentzkow, and C. Yu. 2019. "Trends in the Diffusion of Misinformation on Social Media." *Research & Politics* 6: 1–8.

ARTICLE 19. 2018. "Regulating Social Media: We Need a New Model that Protects Free Expression." London, UK: ARTICLE 19. https://www.article19.org/resources/regulating-social-media-need-new-model-protects-free-expression/.

Aspinwall, N. 2020. "Taiwan's War on Fake News Is Hitting the Wrong Targets." *Foreign Policy*, January 10. https://foreignpolicy.com/2020/01/10/taiwan-election-tsai-disinformation-china-war-fake-news-hitting-wrong-targets/.

Australian Competition and Consumer Commission. 2019. *Digital Platforms Inquiry—Final Report*. Canberra, Australia: Australian Competition and Consumer Commission. https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report.

Benkler, Y., R. Faris, and H. Roberts. 2018. *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*. Oxford: Oxford University Press.

Brüggemann, M., S. Engesser, F. Büchel, E. Humprecht, and L. Castro. 2014. "Hallin and Mancini Revisited: Four Empirical Types of Western Media Systems." *Journal of Communication* 64 (6): 1037–65.

Cederberg, G. 2018. *Catching Swedish Phish: How Sweden Is Protecting Its 2018 Elections*. Cambridge: Belfer Center for Science and International Affairs, Harvard Kennedy School. https://www.belfercenter.org/sites/default/files/files/publication/Swedish%20Phish%20-%20final2.pdf.

Chaykowski, K. 2017. "Facebook Says Fake Accounts Likely Tied to Russia Bought $100,000 in Political Ads." *Forbes*, September 6. https://www.forbes.com/sites/kathleenchaykowski/2017/09/06/fake-facebook-accounts-likely-tied-to-russia-bought-100000-in-political-ads-company-says/.

Christians, C. G., T. Glasser, D. McQuail, K. Nordenstreng, and R. A. White. 2010. *Normative Theories of the Media: Journalism in Democratic Societies*. Champaign: University of Illinois Press.

Coaston, J. 2019. "Sen. Josh Hawley Wants the Government to Police Twitter for Political Bias." *Vox*, June 26. https://www.vox.com/2019/6/26/18691528/section-230-josh-hawley-conservatism-twitter-facebook.

Deibert, R. J. 2018. "Toward a Human-Centric Approach to Cybersecurity." *Ethics & International Affairs* 32 (4): 411–24.

Digital, Culture, Media and Sport Committee. 2018. *Disinformation and "Fake News": Interim Report*. London: House of Commons. https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/363.pdf.

DiResta, R., K. Shaffer, B. Ruppel, D. Sullivan, R. Matney, R. Fox, J. Albright, and B. Johnson. 2018. *The Disinformation Report: The Tactics & Tropes of the Internet Research Agency*. Austin: New Knowledge. https://disinformationreport.blob.core.windows.net/disinformation-report/NewKnowledge-Disinformation-Report-Whitepaper-121718.pdf.

Douek, E. 2018. "What's in Australia's New Laws on Foreign Interference in Domestic Politics." *Lawfare*, July 11. https://www.lawfareblog.com/whats-australias-new-laws-foreign-interference-domestic-politics.

Dryzek, J. S. 2009. "Democratization as Deliberative Capacity Building." *Comparative Political Studies* 42 (11): 1379–1402.

European Commission. 2018a. *Communication from the Commission—Securing Free and Fair European Elections*. Brussels: European Commission. https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-free-fair-elections-communication-637_en.pdf.

European Commission. 2018b. *Tackling Online Disinformation: A European Approach*. Brussels: European Commission. https://ec.europa.eu/digital-single-market/en/news/communication-tackling-online-disinformation-european-approach.

Facebook. 2017. "Information Operations and Facebook." *Facebook Newsroom*, April 27. https://fbnewsroomus.files.wordpress.com/2017/04/facebook-and-information-operations-v1.pdf.

Farrell, H., and B. Schneier. 2018. *Common-Knowledge Attacks on Democracy*. Cambridge: Berkman Klein Center for Internet & Society, Harvard University. https://papers.ssrn.com/abstract=3273111.

Feilzer, M. Y. 2010. "Doing Mixed Methods Research Pragmatically: Implications for the Rediscovery of Pragmatism as a Research Paradigm." *Journal of Mixed Methods Research* 4 (1): 6–16.

Freedom House. 2017. *Freedom on the Net 2017: Manipulating Social Media to Undermine Democracy*. Washington, DC: Freedom House. https://freedomhouse.org/article/new-report-freedom-net-2017-manipulating-social-media-undermine-democracy.

Funke, D. 2018. "Italians Can Now Report Fake News to the Police. Here's Why that's Problematic." *Poynter*, January 19. https://www.poynter.org/fact-checking/2018/italians-can-now-report-fake-news-to-the-police-heres-why-thats-problematic/.

Goodin, R. E., M. Rein, and M. Moran. 2006. "The Public and Its Policies." In *The Oxford Handbook of Public Policy*, ed. R. E. Goodin, M. Rein and M. Moran, 3–35. Oxford: Oxford University Press.

Gould, C. C. 2006. "Self-determination beyond Sovereignty: Relating Transnational Democracy to Local Autonomy." *Journal of Social Philosophy* 37 (1): 44–60.

Government of Canada. 2019. "Combatting Foreign Interference." Democratic Institutions: Backgrounders. https://www.canada.ca/en/democratic-institutions/news/2019/01/combatting-foreign-interference.html.

Government of Denmark. 2018. "Strengthened Safeguards against Foreign Influence on Danish Elections and Democracy." Ministry of Foreign Affairs of Denmark. http://um.dk/en/news/newsdisplaypage/?newsid=1df5adbb-d1df-402b-b9ac-57fd4485ffa4.

Guess, A., B. Nyhan, and J. Reifler. 2018. "Selective Exposure to Misinformation: Evidence from the Consumption of Fake News during the 2016 U.S. Presidential Campaign." *European Research Council*, 9. http://www.ask-force.org/web/Fundamentalists/Guess-Selective-Exposure-to-Misinformation-Evidence-Presidential-Campaign-2018.pdf

Habermas, J. 1996. *Between Facts and Norms: Contributions to a Discourse Theory of Law and Democracy*. Cambridge: MIT Press.

Hallin, D. C., and P. Mancini. 2004. *Comparing Media Systems*. Cambridge: Cambridge University Press.

Henley, J. 2018. "Global Crackdown on Fake News Raises Censorship Concerns." *The Guardian*, April 24. https://www.theguardian.com/media/2018/apr/24/global-crackdown-on-fake-news-raises-censorship-concerns.

High Level Expert Group on Fake News and Online Disinformation. 2018. *A Multi-dimensional Approach to Disinformation*. Luxembourg: European Commission. https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation.

Hollis, D. 2018. "The Influence of War; the War for Influence." *Temple International & Comparative Law Journal* 32:31–46.

Ingram, M. 2020. "Who Is Right about Political Ads, Twitter or Facebook?" *Columbia Journalism Review*, January 16. https://www.cjr.org/the_media_today/political-ads-twitter-facebook.php.

Jeangène Vilmer, J.-B., A. Escorcia, M. Guillaume, and J. Herrera. 2018. *Information Manipulation: A Challenge for Our Democracies*. Paris: Policy Planning Staff, Ministry for Europe and Foreign Affairs, and the Institute for Strategic Research, Ministry for the Armed Forces. https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf.

Karpf, D. 2017. "Sorting through the Facebook-Russia-Trump Advertising Story." *Medium*, September 15. https://medium.com/@davekarpf/sorting-through-the-facebook-russia-trump-advertising-story-d096e3df3edb.

Karppinen, K. 2013. "Uses of Democratic Theory in Media and Communication Studies." *Observatorio (OBS*)* 7 (3): 1–17.

Karppinen, K. 2019. "Freedom without Idealization: Non-ideal Approaches to Freedom of Communication." *Communication Theory* 29 (1): 66–85.

Kaye, D. 2018a. *Mandate of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*. Geneva: Human Rights Council. http://www.ohchr.org/Documents/Issues/Opinion/Legislation/OL-ITA-1-2018.pdf.

Kaye, D. 2018b. *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*. Geneva: Human Rights Council. https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/38/35.

Kreiss, D. R., G. Lawrence, and S. C. McGregor. 2018. "In Their Own Words: Political Practitioner Accounts of Candidates, Audiences, Affordances, Genres, and Timing in Strategic Social Media Use." *Political Communication* 35 (1): 8–31.

Leerssen, P., J. Ausloos, B. Zarouali, N. Helberger, and C. H. de Vreese. 2019. "Platform Ad Archives: Promises and Pitfalls." *Internet Policy Review* 8 (4): 1–21.

Lidberg, J., and D. Muller, eds. 2018. *In the Name of Security: Secrecy, Surveillance and Journalism*. London: Anthem Press.

LSE Commission on Truth, Trust and Technology. 2018. *Tackling the Information Crisis: A Policy Framework for Media System Resilience*. London: London School of Economics and Political Science. http://www.lse.ac.uk/media-and-communications/assets/documents/research/T3-Report-Tackling-the-Information-Crisis.pdf.

MacAskill, E. 2016. "Hostile States Pose 'Fundamental Threat' to Europe, Says MI6 Chief." *The Guardian*, December 8. https://www.theguardian.com/uk-news/2016/dec/08/hostile-states-pose-fundamental-threat-to-europe-says-mi6-chief.

Macron, E. 2018. "IGF 2018 Speech by French President Emmanuel Macron." Internet Governance Forum, November 14. https://www.intgovforum.org/multilingual/content/igf-2018-speech-by-french-president-emmanuel-macron.

Manin, B. 1997. *The Principles of Representative Government*. Cambridge: Cambridge University Press.

Mansbridge, J., J. Bohman, S. Chambers, T. Christiano, A. Fung, J. Parkinson, D. F. Thompson, and M. E. Warren. 2012. "A Systemic Approach to Deliberative Democracy." In *Deliberative Systems: Deliberative Democracy at the Large Scale*, ed. J. Parkinson and J. Mansbridge, 1–26. Cambridge: Cambridge University Press.

Multistakeholder Forum on Disinformation. 2018. *Code of Practice on Disinformation*. Brussels: European Commission. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=54454.

Nakashima, E. 2019. "U.S. Cyber Command Operation Disrupted Internet access of Russian Troll Factory on Day of 2018 Midterms." *The Washington Post*, February 27. https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html.

National Assembly. 2018. "Organic Law No. 2018-1201 and No. 2018-1202 of 22 December 2018 Relating to the Fight Against Information Manipulation." Paris: National Assembly.

NATO StratCom. 2016. *Social Media as a Tool of Hybrid Warfare*. Riga, Latvia: NATO Strategic Communication Centre of Excellence.

Nielsen, R. K., and L. Graves. 2017. *"News You Don't Believe": Audience Perspectives on Fake News*. Oxford: Reuters Institute for the Study of Journalism. https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2017-10/Nielsen&Graves_factsheet_1710v3_FINAL_download.pdf.

Ohlin, J. D. 2017. "Did Russian Cyber Interference in the 2016 Election Violate International Law?" *Texas Law Review* 95 (7): 1579–98.

Osnos, E. 2018. "Can Mark Zuckerberg Fix Facebook Before It Breaks Democracy?" *The* New Yorker, September 10. https://www.newyorker.com/magazine/2018/09/17/can-mark-zuckerberg-fix-facebook-before-it-breaks-democracy

Pamment, J., H. Nothhaft, H. Agardh-Twetman, and A. Fjällhed. 2018. *Countering Information Influence Activities: The State of the Art*. Lund: Swedish Civil Contingencies Agency (MSB) and Lund University. https://www.msb.se/RibData/Filer/pdf/28698.pdf.

Paul, C., and M. Matthews. 2016. *The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It*. Santa Monica: RAND Corporation. https://www.rand.org/pubs/perspectives/PE198.html.

Pomerantsev, P. 2019. *A Cycle of Censorship: The UK White Paper on Online Harms and the Dangers of Regulating Disinformation*. Amsterdam: Transatlantic High Level Working Group on Content Moderation Online and Freedom of Expression. https://www.ivir.nl/publicaties/download/Cycle_Censorship_Pomerantsev_Oct_2019.pdf

Przeworski, A. 1999. "Minimalist Conception of Democracy: A Defense." In *Democracy's Values*, ed. I. Shapiro and C. Hacker-Cordón, 23–55. Cambridge: Cambridge University Press.

Puppis, M. 2014. "The Regulation of Political Communication." In *Political Communication*, ed. C. Reinemann, 39–61. Berlin: Walter de Gruyter GmbH.

Schudson, M. 1998. *The Good Citizen: A History of American Civic Life*. New York: Free Press.

Schumer, C. 2019. "Executive Session; Congressional Record Vol. 165, No. 79." U.S. Government Publishing Office. https://www.congress.gov/congressional-record/2019/5/13/senate-section/article/s2776-2?s=1&r=12.

Smith, R. C. 2019. "Fake News, French Law and Democratic Legitimacy: Lessons for the United Kingdom?" *Journal of Media Law* 11 (1): 52–81.

Spaulding, S., D. Nair, and A. Nelson. 2018. "Why Putin Targets Minorities." Washington, DC: Center for Strategic & International Studies. https://www.csis.org/analysis/why-putin-targets-minorities.

Stocking, G. 2019. "Many Americans Say Made-Up News Is a Critical Problem that Needs to Be Fixed." *Pew Research Center*, June 5. https://www.journalism.org/2019/06/05/many-americans-say-made-up-news-is-a-critical-problem-that-needs-to-be-fixed/.

Taiwan Foundation for Democracy. 2019. "TFD Survey on Taiwanese View of Democratic Values and Governance." Taiwan Foundation for Democracy. http://tfd.org.tw/export/sites/tfd/files/news/pressRelease/0719_press-release_web.pdf.

Tenove, C., and S. McKay. 2019. "Online Disinformation and Systemic Threats to Democratic Deliberation." Paper presented at the International Studies Association Annual Conference, Toronto, Canada, March 27-30.

Tenove, C., and H. J. S. Tworek. 2019. "Online Disinformation and Harmful Speech: Dangers for Democratic Participation and Possible Policy Responses." *Journal of Parliamentary and Political Law* 13:215–32.

Tworek, H. J. S., and P. Leerssen. 2019. *An Analysis of Germany's NetzDG Law*. Amsterdam: Transatlantic High Level Working Group on Content Moderation Online and Freedom of Expression. https://www.ivir.nl/publicaties/download/NetzDG_Tworek_Leerssen_April_2019.pdf.

United Kingdom Parliament. 2019. "Secretary of State for Digital, Culture, Media & Sport and the Secretary of State for the Home Department." Online Harms White Paper. https://www.gov.uk/government/consultations/online-harms-white-paper.

Vaidhyanathan, S. 2019. "Why Conservatives Allege Big Tech Is Muzzling Them." *The Atlantic*, July 28. https://www.theatlantic.com/ideas/archive/2019/07/conservatives-pretend-big-tech-biased-against-them/594916/.

Verza, S. 2018. "Tackling Fake News, the Italian Way." Resource Centre on Media Freedom in Europe. http://www.rcmediafreedom.eu/Tools/Legal-Resources/Tackling-fake-news-the-Italian-way.

Wardle, C., and H. Derakhshan. 2017. *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making*. Report DGI(2017)09. Strasbourg: Council of Europe. https://firstdraftnews.com/wp-content/uploads/2017/10/Information_Disorder_FirstDraft-CoE_2018.pdf?x56713.

Warren, M. E. 2017. "A Problem-Based Approach to Democratic Theory." *American Political Science Review* 111 (1): 39–53.

Watts, D. J., and D. M. Rothschild. 2017. "Don't Blame the Election on Fake News. Blame It on the Media." *Columbia Journalism Review*, December 5. https://www.cjr.org/analysis/fake-news-media-election-trump.php.

Woolley, S. C., and D. Guilbeault. 2018. "United States: Manufacturing Consensus Online." In *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media*, ed. S. C. Woolley and P. N. Howard, 185–211. Oxford: Oxford University Press.

Young, I. M. 2000. *Inclusion and Democracy*. Oxford: Oxford University Press.

Ytre-Arne, B., and H. Moe. 2018. "Approximately Informed, Occasionally Monitorial? Reconsidering Normative Citizen Ideals." *The International Journal of Press/Politics* 23 (2): 227–46.

Author Biography

Chris Tenove is a postdoctoral fellow in the Department of Political Science at the University of British Columbia.