DIGITAL AUTHORITARIAN THREATS TO UNITED STATES' DEMOCRACY

Digital Authoritarianism Group Policy Report
POLSCI 765: Digital Threats to Democracy
Shannon Dales, Rebecca Denyer,
Brenna Friesen, Ryan Hart, and Rida Mohsin
Drs. Tony Porter and Netina Tan
April 7, 2021
Word Count: 6,807

Table of Contents

Executive Summary

Digital authoritarianism is on the rise globally, and democracies such as the United States are not immune to these influences. This policy report utilizes several case studies that demonstrate digital authoritarianism's impact on American democracy at the state, corporate, and individual levels. Within these levels of analysis, the theoretical frameworks of sharp power and digital systems of oppression provide useful ways of understanding digital authoritarianism's effects on democratic values and freedoms. Authoritarian threats to American state-level institutions and state security measures are becoming more prominent as autocratic regimes project their sharp power in cyberspace and democracies incorporate digital surveillance practices that further entrench institutionalized systems of oppression. American tech companies have increasingly divorced their interests from the state, pursuing growth at the expense of liberal democratic values; as a result, these companies have supported the development of autocratic surveillance and control technologies. Individual user experience on online platforms is an extension of civil liberties, specifically the freedom of expression and speech. While the protection of democratic values within online spaces is crucial in combating digital authoritarian tendencies, the American federal government has been complacent in the perpetuation of oppression online. Current regulations and policy models have been unable to effectively address 1) the long-term ramifications of authoritarian influences on American democracy, 2) the US's increasing normalization of digital authoritarianism practices, and 3) the continued degradation of Americans' civic rights and freedoms. Due to the failure to address the aforementioned gaps and the absence of guidelines, it is crucial to implement the proposed policy recommendations in this report.

Introduction

The global decline of democratic values presents a growing challenge for democracies, demonstrating the prematurity of the optimism surrounding the third wave of democratization (Lührmann and Lindberg 2019, 1096). Digital authoritarianism (DA) can be broadly defined as the "use of digital tools to surveil, repress, and manipulate domestic and foreign populations" (Tan 2021; Polyakova and Meserole 2020, 1). In particular, DA presents an increasing threat to United States (US) national security and democracy (Sherman 2021, 107). Hacking American political institutions has become a prominent method authoritarian regimes use to erode democratic values and manipulate foreign democratic populations, thereby contributing to the spread of DA (Rid and Buchanan 2018, 8). In their pursuit of profit, American tech corporations have disregarded fundamental human rights, thereby validating authoritarian regimes and the China Model as a legitimate alternative to development. The use of facial recognition technology (FRT) by American law enforcement presents concerns on how this technology infringes on democratic freedoms and reproduces digital racial oppression through the normalization of state digital authoritarian surveillance practices. Lastly, current content regulation often silences certain voices while allowing others to thrive on digital platforms, which facilitates the rise of authoritarian censorship within democracies (Angwin and Grassegger 2017). Online intimidation and harassment within social media platforms also carry the potential to negatively impact political participation and create new barriers to entry as activists and political candidates have come under attack from trolling campaigns and death threats. In conclusion, DA is infiltrating American democracy in a multitude of ways, and this policy report will provide guidance and policy recommendations for the US federal government to curb its continued propagation.

This policy brief will explore the following questions to determine appropriate policy recommendations: How are authoritarian government-directed hacking and authoritarian government relationships with American corporations undermining democratic values and contributing to the spread of DA? How do DA and systems of oppression become integrated into democratic societies through the use of emerging technologies both by private corporations, platform users, and state actors? Through the examination of a series of case studies, this policy brief will pose the arguments that follow. Authoritarian governments' hacking activities against American federal, democratic institutions is weakening public trust in these institutions. This erosion of trust is further exacerbated by the divorce of interests between the state and the corporation; this results in American firms becoming complicit in the violation of human rights, thereby raising the validity of the China Model, and undermining American soft power. Furthermore, authoritarian techniques are increasingly being utilized within democracies, which is reflected in the private technology sector, digital platforms, and state governance in the US. These strategies include undermining personal privacy and public trust by perpetuating systems of oppression through public digital platforms and state surveillance technology. Finally, policy recommendations will be provided based on the research findings outlined in this report.

Literature Review

Digital Authoritarianism, Sharp Power, and Democracy

DA is a prominent threat to American democratic state institutions, and it has often been propelled by American corporations and spread through authoritarian influence on democracies.

Authoritarian states engage in hacking activities against democracies, such as the US, for reasons that include influencing elections, undermining political institutions, exacerbating extremism, and committing strategic espionage (Kerr 2018, 61). Additionally, because many advanced technologies can be used for both tyrannical and democratic purposes, American companies supply a significant proportion of the surveillance and censorship technologies autocratic countries utilize to control their populations (Sherman 2021, 110). Furthermore, as autocratic regimes such as China and Russia become the top global suppliers of digital technologies and ICT infrastructure useful for advancing authoritarianism, they are developing more sophisticated sharp power capabilities (Polyakova and Meserole 2020, 1, 9). Sharp power is associated with authoritarian regimes' aggressive and malign efforts to stealthily exploit the open nature of democratic institutions while avoiding detection (Walker and Ludwig 2017, 13). As an outward expression of DA, sharp power describes Chinese and Russian exercises of power that the soft power/hard power dichotomy could not capture (Walker and Ludwig 2017, 12). Hard power relies on coercive military and economic measures while soft power is exercised non-coercively when states convince other states to desire what they want, through utilizing the power of ideas, for example (Nye 1990, 164, 166). In the digital age, sharp power presents a particularly menacing threat to democracies' open and accessible cyberspaces.

Authoritarian state-backed hacking is a form of foreign interference against democracies that represents a general avenue through which autocratic states project sharp power and DA (Henschke, Sussex, and O'Connor 2020, 181–82; Rid and Buchanan 2018, 8). Foreign interference activities are most damaging to democracies when they target one of the following "five I" vulnerabilities: democratic *institutions*, private *industry*, election *infrastructure*, core democratic *ideas* and norms, and *individuals* (Henschke, Sussex, and O'Connor 2020, 181). Democratic institutions are the most prominent targets for authoritarian hackers, whose efforts have created significant fissures in social cohesion (Rid and Buchanan 2018, 8). In particular, the public trust these institutions rely on for their legitimacy is the major democratic value authoritarian hackers attempt to undermine, demonstrating a significant source of sharp power (Arpino and Obydenkova 2020; Rid and Buchanan 2018, 8). Democracies require public trust because "it is considered a necessary precondition for democratic rule, [and] a decline in trust is thought to fundamentally challenge the quality of representative democracy" (van der Meer 2017, 1). Not coincidentally, the core democratic value present in all five I's is public trust in democracy (Henschke, Sussex, and O'Connor 2020, 183). Maintaining public trust in democracy is vital to its preservation, which requires stronger protection of critical democratic institutions against cyberattacks from autocracies.

The absence of morality in the corporate pursuit of profit has resulted in the undermining of democratic values and ideals as American firms attempt to penetrate the Chinese market. (Crofts and van Rijswijk 2020, 80; Liu 2021, 54). To access the market, American companies have had to conform to Chinese regulations and data localization policies, subjecting them to the scrutiny and control of the CCP (Liu 2021, 52). Despite broader liberalization efforts made within China, companies are expected to operate for the benefit of the state and its agenda (Freedman, 2021). This realignment of goals (officially referred to as the prevention of "the disorderly expansion of capital") has been at the heart of recent trust-busting measures made by the CCP (Freedman 2021). With the American tech sector complicit in its DA practices, the CCP can more effectively direct the expansion of its sharp power capabilities while promoting the development of its own AI sector through extensive data sets unavailable to competitors. (Liu 2021, 48; Darby and Sewall 2021).

China's state-corporate relationship places disproportionate weight on the state, emphasizing innovation and control over capital growth to further the grand ambitions of the CCP.

Digital Authoritarianism and Systems of Oppression Within Democracies

Understanding how digital oppression is exacerbated within Internet and technology infrastructures requires an expansive look into corporate regulation of user speech and state-led use of surveillance technologies (Gangadharan 2021, 113). This understanding of digital systems of oppression is rooted in institutional power and histories of inequality, which results in technological practices that disproportionately affect racialized communities while further infringing on democratic rights and freedoms (NMAAHC 2019). The growing concerns over the expansive reliance of DA practices within democratic states has resulted in the pressing need for effective policies to protect the rights and privacy of all Americans.

With this in mind, the US law enforcement's use of FRT presents one concerning way government officials are using DA tactics to retain power and control of the public's personal data (Michaelsen and Glasius 2018; Silverman 2017). Extensive and untargeted use of this technology raises concerns over FRT's long-term effects and how the lack of regulation "undermine[s] fundamental rights, in particular the right to privacy, and may lead to prejudice and discrimination" (Nesterova 2019, 1; Yayboke and Brannen 2020). With the US Department of Justice's introduction of the Smart Policing Initiative of 2017, local police units received increased funding for technological innovation that included FRT (Smart Policing Initiative 2017; Ringrose 2017, 57). With approximately half of all American adults' data being store in country-wide facial recognition databases, concerns over this technology's extensive use have become even more dire considering the recent studies on software inaccuracies regarding Black faces and the biases and ethical dilemmas ingrained within technological development (Ringrose 2017, 58; Leslie 2020). Thus, further federal and state-wide policies and regulations need to be developed to prevent the continuing effects that FRT has on democratic freedoms and privacy rights in the US.

Furthermore, the prevalence of hate speech on digital platforms is one of the many ways individuals within democracies attempt to utilize authoritarian techniques. Free speech is a right granted in the US by the First Amendment (U.S. Const. amend. 1). However, digital platforms such as Facebook are not bound by the Constitution's First Amendment and have thus shaped a new system of governance where platforms can control what information exists in the public sphere (Kadri and Klonick 2019). Many scholars have noted inconsistencies in how platforms regulate hate speech and digital harassment. This is felt along the ideological spectrum and can particularly be attributed to faulty decision models developed by media platforms like Google, Twitter and Facebook (Brunk et al. 2019, 1). Therefore, it is important to consider how hate speech exists on digital platforms, the effect this has on US democracy, and what digital platforms are doing to combat hate speech.

Furthermore, there has been an ongoing rise of right-wing hate groups within online spheres, which is believed to be mirroring the recent rise of right-wing populism instigated by Trump and other similar figures in politics (Marshak 2017, 506). The growth of right-wing rhetoric and targeted online attacks have been further intensified based upon the imagined binary of populist ideals towards forming an 'us' vs 'them' adversarial grouping (Saresma et al. 2021, 224). Furthermore, despite Facebook's ban of hate speech under their Community Guidelines, scholars argue right-wing groups have instead found ways to continue to spread violent speech without being flagged or removed by Facebook (Ben-David and Matamoros-Fernández 2016; Ghosh

2020). Users have discovered specific language that does not result in them being flagged by human or AI moderators, and have strategically utilized the under-regulated comments sections to spread digitally mediated violence (Ben-David and Matamoros-Fernández 2016; Saresma et al. 2021, 224). The term 'digitally mediated violence' refers to the harm presented within online harassment towards its targets as well as broader ideological movements that are intensified as violence is promoted to address constructed enemies (Saresma et al. 2021, 224). Furthermore, Facebook's "like," "share," "comment," and "report" buttons also provide resources to hate groups, as these groups create echo chambers of ideas, which are fueled by obtaining likes, gathering numerous comments, and challenging other users to report them (Ben-David and Matamoros-Fernández 2016, 1168; Ghosh 2020; Sunstein 2017). Therefore, digital platforms are reproducing systems of oppression, as the issue lies not only with user's speech, but also with the affordances of the platforms and how these digital platforms regulate hate speech.

Case Studies

Case Study 1: Digital Threats to Democratic State Institutions

Hacking democratic states' political institutions is one of many foreign interference methods authoritarian governments use to undermine American trust in democracy (Omand 2018, 10). Americans' declining trust in government makes their political institutions desirable targets for authoritarian foreign interference (Rid and Buchanan 2018, 8). Two cases of hacking in 2015 against the Office of Personnel Management (OPM) and the Internal Revenue Service (IRS) demonstrate the American federal government's vulnerabilities to DA. In April 2015, a Chinese state-sponsored group breached the OPM's network (Chen 2019, 3). The data breach compromised 21.5 million peoples' sensitive information, including that of 4.2 million federal employees, their background checks, and federal security clearance questionnaires (Chen 2019, 3–4; Vail 2017, 221). In May 2015, it was publicized that Russia had breached nearly 700,000 taxpayer accounts through the IRS between January 2014 and May 2015 (Huffpost 2015; New York Post 2015; Morgan 2016; IRS 2016). Previously stolen taxpayer information from non-IRS sources was used to file fraudulent tax returns and between $39 and $50 million was stolen via these dishonest tax returns (Chen 2016, 104; Reisinger 2015). To curb Americans' deteriorating trust in democracy, it is necessary to protect their federal institutions more effectively from authoritarian governments' cyberattacks.

Both cyberattacks demonstrate a perfect recipe for undermining democracy and reveal American political institutions' vulnerability to authoritarian influence in cyberspace. The consequences of these cyberattacks for American democracy are demonstrated by the associated threats to national security and Americans' trust in democratic institutions. As the primary personnel manager and human resources agency for the US federal government, the OPM represents a core democratic institution tasked with ensuring the American democracy operates effectively (OPM 2021), demonstrating the importance of maintaining public trust in this democratic institution. Additionally, the IRS faces enormous challenges with maintaining public trust as they increasingly struggle with taxpayer identity theft (Falsetta 2020, 79). Given taxation legitimacy's close association with democratic representation in the US (Kato and Tanaka 2018, 184), decreased trust in this institution signals a detriment to democratic values. The IRS and OPM attacks have highlighted the American government's ineptitude in protecting key democratic institutions and civilians' personal data, which has citizens justifiably worried about whether they

can trust government agencies to protect their data and secure the institutions they trust (Gootman 2016, 522). Furthermore, while the US values the open flow of information and ideas, their resistance to regulating cyberspace disadvantages them because authoritarian governments exploit this openness through cyberattacks and data breaches (Rosenberger 2020, 146; Schmidt et al. 2019, 19). This creates national security threats because of the declining public trust in American political institutions and the fact that the stolen information can be weaponized against the US government (National Security Agency 2021; Gootman 2016, 522). In sum, authoritarian governments' cyberattacks against America's political institutions pose grave national security risks and undermine public trust, which is necessary for any democracy.

The domestic policy and regulatory context is critical to understanding opportunities to enhance US political institutional security. The IRS is entrusted with providing Americans "top quality service" and fairly enforcing taxation laws (IRS 2020a), while the OPM is responsible for providing "a secure employment process," as well as helping the federal government serve the American people (OPM, 2021). Several organizations hold the IRS and the OPM accountable. The *Budget and Accounting Act of 1921* established the Government Accountability Office (GAO) (67th Congress 1921), which is tasked with providing oversight for the IRS and OPM (IRS 2020b; GAO 2021). In addition, the *IRS Restructuring and Reform Act of 1998* created the Treasury Inspector General for Tax Administration (TIGTA) "to provide independent oversight of IRS activities" (105th Congress 1998; TIGTA, 2020). Additional oversight of the OPM is provided through the OPM Inspector General's office, which was created with the *OPM IG Act of 2014* (113th Congress 2014). Despite presenting an appearance of accountability, these oversight agencies are unable to enforce information security measures within the OPM and IRS, as demonstrated by the multitude of outstanding recommendations for both agencies (GAO 2021; TIGTA 2020; OPM IG, 2018). For example, the OPM has yet to create a policy that mandates annual organization-wide cybersecurity risk assessments and does not provide specialized training for individuals with significant security responsibilities (GAO 2016; 2019; OPM IG, 2018). The IRS does not conduct risk assessments of the various authentication channels to reduce identity theft and has many shortcomings in the implementation of its information security program (GAO 2015; 2017; 2018a; 2018b). The inadequacy of existing policies and practices for securing American democratic institutions must be addressed.

Case Study 2: Corporate Compliance in Authoritarian Practices

In their pursuit of profit, tech corporations have become compliant with authoritarian regulatory practices, and therefore complicit in their violation of liberal democratic ideals. With one of the fastest growing consumer markets and a quickly expanding tech sector, China's potential makes it highly desirable for companies to gain a foothold (Atsmon et al. 2012, 15). China's regional investments in digital infrastructure through the Belt and Road Initiative (BRI)- an ambitious project connecting China to Africa and Europe emulating the Silk Roads of antiquity- further raise the long-term growth potential of the region, intensifying their sphere of influence and coercive abilities (Cheney 2019, 1; Shen 2018, 2684-2685). Fears have arisen that China will utilize this leverage to promote the spread of DA to BRI member states (Polyakova and Meserole 2019, 6; Hemmings 2020, 6); however, while China enables regimes seeking access to autocratic technologies, it claims not to encourage the spread of its ideology (Weiss 2019; Bader, Grävingholt, and Kästner 2010, 90). At the forefront of China's digital infrastructure lies the BeiDou Satellite constellation, a technological rival to American GPS since it surpasses American

precision capabilities (Woo and Gao 2020). To promote greater regional integration, the Chinese Communist Party (CCP) has encouraged BRI member states to adopt the use of its system, further splintering the region from American influence (Cheney 2019, 6). The American influence that remains has persisted within its firm's operations; however, the influence has been divorced from the reach of the state. In their quest for access, these corporations have aided the CCP in the development, preservation and export of its surveillance and control apparatus.

There does not currently exist any substantial or binding regulations that limit corporate-state partnerships with authoritarian (or democratic) states (Matthews and Tsagaroulis, 2020). Further, the trade in control/surveillance technologies is often classified as commercial, rather than military, allowing relatively free movement of these technologies from democracies to authoritarian regimes (Schaake 2020). Within authoritarian states, emerging data localization policies require that companies transfer data to state servers, which then becomes integrated into the state surveillance apparatus (Liu 2021, 52). Since these surveillance and control technologies are being applied for autocratic repression, democratic states must ensure their corporations uphold liberal values to avoid infringement of democratic ideals.

In August of 2018, the Intercept published leaked documents revealing Google's plan to release a censored version of its platform, codenamed Dragonfly, which conformed to standards the CCP set (Gallagher 2018). Since Google's removal from Chinese cyber-domains in 2014, innovation has taken a toll within China (by approximately 8%) leading to a renewed desire for platform access within China, and the desire to fulfil that market demand from the company (Zheng and Wang 2020, 2235). As one of the most prolific tech firms globally, Google's compromise on human rights for the CCP has negative consequences of setting of a new precedent for tech firms internationally and the potentially devastating effects of emerging democracies adopting similar systems (Gallagher 2018). Technology has long held a significant role within China for cementing political stability, and its application of AI technology is no exception (Liu 2021, 64; Neubert and Montañez 2020, 197). Although the company took a step back from Dragonfly following public outrage in 2018, it is likely they will resume the project once the spotlight dims, as they have done in the past when faced with public resistance (Gallagher 2019; Zuboff 2019, 156–57). Google's grand ambition for becoming the default global search engine does not end with China and is likely to permeate into the Global South via the BeiDou system.

The BeiDou system symbolizes a major technological milestone for the CCP in its attempted ascent to regional hegemony (Cheney 2019, 6). BeiDou provides the People's Liberation Army, and any other regime which adopts it, satellite capabilities free from any potential American eavesdropping or counter-intervention (Goswami 2020). In the Pacific region, BeiDou offers precision targeting capabilities down to 10cm, compared to GPS' 30cm, swaying the advantage towards China's military allies (Goswami 2020; Woo and Gao, 2020). In addition to promoting uptake to BRI member states, China has offered BeiDou's services to any state or company at no charge, significantly increasing the potential of states to integrate themselves with global markets. It should be noted, however, that through BeiDou, Chinese presence, implicitly or explicitly, will increase substantially within its sphere of influence (Goswami 2020). BeiDou also presents China with the potential to access even more training data for its AI, placing its tech sector in an advantageous position against American companies in the long-term (Hemmings 2020, 6; Liu 2021, 49-50). While it might not claim to encourage the spread of authoritarianism to its neighbours, the CCP stabilizes autocratic regimes and enables the repression of their domestic populations (Bader, Grävingholt, and Kästner 2010, 88-91). BeiDou and the digital BRI carries the potential of lifting millions of people out of poverty and integrating them into the global

economy; however, following the China Model of development risks autocratizing the region and solidifying Chinese regional hegemony. It is therefore in American geostrategic interest to preserve liberal democratic values and impede the spread of DA; otherwise, it will find its interests in the Global South relegated to those of China.

Case Study 3: Digital Threats by Law Enforcement on Democratic Freedoms

The recent concerns over how digital technology has threatened civil rights and freedoms are not solely regarding foreign influence from authoritarian regimes, but also includes concerns over how this technology erodes democratic states through their participation in authoritarian actions (Michaelsen and Glasius 2018, 3789). To understand how systems of oppression exist within these digital technology infrastructures, it is crucial to examine the ways that software such as FRT have inbuilt racial biases within the software that fail to accurately recognize Black faces (NMAAHC 2019; Garvie and Frankle 2016). With this in mind, the American law enforcement's unregulated use of this flawed technology is founded on the desire for mass collection and control of citizen data, which only further violates the privacy and democratic freedoms of the American people (Silverman 2017, 149). In recent years, the US law enforcement's use of FRT has raised concerns from lawmakers, scholars, NGOs, and technology firms about the lack of regulation over this technology and the long-term effects of its use by state security. Debates surrounding algorithmic inaccuracies, racial biases and privacy violations present implications on the potential impacts these technologies have on democratic freedoms and the ways the US criminal justice system will use this unregulated data (Gravie and Frankle 2016; Klare et al. 2012). Studies have shown that inaccuracies in commonly used FRTs such as Amazon's Rekognition Scan and ClearviewAI, specifically impact racialized Americans due to biases and algorithmic errors, which has led technology companies and lawmakers to raise concerns about the long-term consequences of the lack of effective policy responses (Hill 2021; Valentino-DeVries 2020; Markey 2020). Over the past year, corporations like Microsoft, IBM, and Amazon began a moratorium on the selling of their FRT to law enforcement due to these concerns and have since advocated for the US government's formal regulation of these technologies (Duffy 2020; Jackson 2020).

While discussions surrounding federal legislative measures on the topic continue, over 600 American law enforcement agencies continue to use FRT in 2020 (Valentino-DeVries 2020). In California and New York, there have been debates by both lawmakers and NGOs surrounding local police's arbitrary use of FRTs. Both Amnesty International and the ACLU continue to advocate for state examination into whether FRT is necessary for day-to-day policing and they state the importance of developing regulations on law enforcement's use of the technology (Hern 2021). Despite New York's recent discussions on implementing legislation surrounding the NYPD's use of surveillance technology, the state continues to lack effective regulations on the department's use of FRT and instead, they restricted their legislation to solely reporting and evaluating general surveillance software (Jackson 2021). Likewise, the LAPD's use of FRT has made significant expansions into various forms, from the software's inclusion in their 2016 "smart cars" to their extensive use of facial recognition databases for small crimes (Garvie and Frankle 2016; Rector 2021). Earlier this year, the LAPD approved a policy to present limitations on what software they can use but they still fail to effectively regulate the accepted usage, leading to concerns about the embedded software flaws that disproportionately affect Black Americans (Rector 2021; Klare et al. 2012). Unlike both New York and California, Massachusetts' new bill S.2963 includes regulations on FRT's use, legal permission requirements for the technology's use,

as well as the inclusion of an app that only the state police or FBI can use, not local officers (Hill 2021; 192nd General Court of the Commonwealth of Massachusetts 2020). This policy has been praised by members of the ACLU who recognize the impossible nature of a full ban on FRT and consider Massachusetts' new regulations as a positive step forward in state-made legislation on FRT (Ibid).

All three of these states present tangible case studies that contribute to the potential for policy solutions and regulations on FRT at both a federal and state level. In conjunction to state-led policies, members of Congress have recently been arguing for stricter legislation regarding federal and local law enforcement's use of these technologies and the lack of action, which has disproportionately affected racialized communities (Markey 2020; Newman 2019). Last year, the *Facial Recognition and Biometric Technology Moratorium Act of 2020* was introduced to Congress to halt federal and local law enforcement's use of FRT (Markey 2020). If passed, this Act would represent a significant milestone in policy production that aims to protect Americans' civil rights and freedoms and recognizes the ways law enforcement engage in undemocratic initiatives with this technology, which further reinforces systematic oppression.

Case Study 4: Facebook's Contribution to Authoritarian Practices

Content regulation on Facebook has been criticized for facilitating the rise of authoritarian censorship within democracies through unclear regulation policies and digital systems of oppression that often silence certain voices while allowing others to thrive on their platform. There are several federal laws in the US that address social media regulation; however, most address privacy concerns and not the regulation of hate speech online. The primary federal law that currently addresses hate speech online is the *Communications Decency Act* (*Electronic Frontier Foundation* n.d.). However, content on social media remains primarily regulated by the individual technology companies, which users agree to during registration. Facebook specifically touches upon content moderation and the regulation of hate speech in their Community Standards under "Objectionable Content" (*Facebook Community Standards* 2021). Overall, Facebook states that any direct attacks against individuals based on human characteristics are considered hate speech (*Facebook Community Standards* 2021).

Facebook's community standards define hate speech as an attack on a person within a protected category, but what does "protected category" mean (*Facebook Community Standards* 2021; Angwin and Grassegger 2017)? Some protected categories include race, ethnicity, nationality, sex, gender identity, and disability (*Facebook Community Standards* 2021). However, in 2017, American congressman Higgins called for the slaughter of "radicalized" Muslims in a Facebook post, which was left posted for public consumption (Angwin and Grassegger 2017). Facebook's internal documents for content moderation show that since Higgins used the word "radicalized," the post passed community guidelines since it was not an attack on a full racial group, but rather a specific sub-group (Angwin and Grassegger 2017). For a group to be protected from hate speech, all the listed traits in the Facebook post must fit into a protected category. However, in Higgins' post, the characteristic "radicalized" is not a protected trait, so the post does not violate Facebook's hate speech rules.

Furthermore, many Black Lives Matter activists have complained after Facebook removed their posts about White supremacy and violence against Black Americans. Despite Facebook acknowledging in their Community Standards that speech on Facebook is sometimes used in an exemplary way to show the kind of discrimination that minority groups face, Facebook has still

removed many individual's posts quoting or showing photos of racist messages they have received (*Facebook Community Standards* 2021; Guynn 2019). On June 3, 2020, activist Louiza Doran was notified that any post that had her name, was linked to her work, or even included her picture had been flagged and removed for violating Facebook's community standards (Silverman 2020). Doran explained that her content was often removed, and her account was sometimes suspended due to her frequent discussion of Black individuals' experiences with systematic racism.

Many activists do not want to support Facebook and its guidelines; however, they also acknowledge Facebook is the best place to spread information on events and reach large groups of people. Activist Carolyn Wysinger stated that Facebook views racist speech as "simply a matter of a difference of opinion" (Silverman 2020, para. 15). Wysinger has also had her posts removed by Facebook, such as a reposted quote that read, "On the day that Trayvon would've turned 24, Liam Neeson is going on national talk shows trying to convince the world that he is not a racist," and added her own text that read, "White men are so fragile, and the mere presence of a black person challenges every single thing in them" (Guynn 2019, paras. 2-4; Rice 2020; Levy 2020). Facebook deleted Wysinger's post in only 15 minutes for violating its standards for hate speech, and she was given a warning that if she posted anything like this again, her account would be deactivated for 72 hours (Guynn 2019).

Finally, Black Lives Matter organizer Tanya Faison had a post removed due to hate speech, which read, "Dear white people… it is not my job to educate you or to donate my emotional labor to make sure you are informed. If you take advantage of that time and labor, you will definitely get the elbow when I see you" (Guynn 2019, para. 12). On the other hand, another user posted a photo of Faison accompanied by text stating their wish for someone to murder her (Levy 2020). This Facebook post remains untouched by content moderators (Levy 2020). Lastly, it is important to acknowledge that this kind of violent speech online has been cited as directly affecting real-world violence against minorities (Scott and Delcker 2019; Siripurapu and Merrow 2021). Overall, Facebook's community standards lack clarity pertaining to protected and unprotected groups. There also continues to be issues concerning the presence of hate speech and the removal of speech that is trying to bring light to the racism that exists both on and off the platform. All these issues are contributing to the rise of DA within the US, as certain voices and ideas are permitted to exist on Facebook while other ideas are being silenced.

Case Study 5: Online Harassment as a Threat to Democracy

The unfettered nature of online discourse on platforms such as Facebook and Twitter has facilitated a toxic environment for women and emboldened harassment and trolling, which can replicate systems of oppression that exist in given social structures. This phenomenon has made it increasingly harder for women in politics to strategically make use of such platforms, thereby enabling political intimidation and facilitating DA. Online harassment is cited as a barrier to entry for many considering a career in politics given the severity of the abuse often levied against those that do enter politics (Krook and Sanin 2019, 740). Existing female politicians are also unable to communicate with constituents efficiently due to constant interaction with internet harassers that flood comment sections and inboxes. There is a clear consensus that women in general are targeted at a higher rate and young women are more vulnerable than older adults in the escalation of online harassment towards attempted physical harm (Marshak 2017, 506).

In recent years, especially since the 2016 American elections, online harassment has steadily grown along with populist rhetoric (Marshak 2017, 506). Female political candidates have

experienced online harassment throughout their campaigns, and some continue to be harassed long afterwards. The case of Erin Schrode exemplifies this; Schrode was a congressional candidate for California during the 2016 elections who faced immense online harassment containing sexist, abusive, and anti-Semitic remarks (Mekouar 2019). The harassment was further instigated by a neo-Nazi website that led a trolling campaign against Schrode, which also released her personal phone number and email address (Mekouar 2019). The targeted harassment of Schrode did not end after she had lost her primaries and continued well into 2018 (Astor 2018).

Internet trolls often target women of colour and women from minority groups (Astor 2018), thereby reproducing systems of oppression online. In terms of gendered online hate, "the more these categories intersect in any single individual, the more likely any public appearance or visible activism on their part will result in targeted hate toward that individual" (Saresma et al. 2021, 222). Therefore, women in general and women from minority groups are at a greater risk of experiencing similar societal structures of violence on online platforms. Schrode was clearly targeted not only as a woman, but also as a Jewish woman. Attacks on racial, religious, and ethnic identity are clearly motivating factors within online hate and harassment. Ilhan Omar, a current House Representative for Minnesota, is one of the most demonstrative cases of hate speech and harassment being specifically targeted at a candidate because of their gender, race, and religion. As a Black woman, Omar was subject to racist comments, and as a Muslim woman, she faced substantial backlash. This harassment was exacerbated by President Trump as he called Omar out in his tweets and portrayed her in a negative light (Saresma et al. 2021, 232-233). Similarly, House Representative for Massachusetts, Ayanna Pressley, was also the victim of online harassment and hate speech directed towards her gender and race (Haines 2021). Omar and Pressley are both current members of Congress and face online trolls and negative comments daily. The examples of their struggles online can discourage women, especially women of colour, from participating in politics. The 2016 elections also marked the first instance of a female candidate dropping out of a race due to an influx of death threats and online harassment. Kim Weaver ran in Iowa's congressional race in 2016 but decided to withdraw from the race after she felt that her personal safety was at risk due to online harassment and threats on her life (Doyle 2017). Weaver's case is also demonstrative of political intimidation online to suppress political participation.

Though content moderation methods and restriction attempts have been made, issues have risen over ineffectual moderation or unequal application of policies. Users, and politicians themselves, have noted the discrepancies between responses to trolls attacking female politicians and other claims of harassment (O'Sullivan 2020). At present, users can block unwanted accounts from interacting with them and platforms like Twitter and Facebook have their own internal policies for regulation. This current form of regulation is reliant on other users flagging inappropriate content and reporting it under the applicable violation (Ullmann and Tomalin 2019, 73). The main cause of concern for women on these online platforms is the security of their private information and the ability to safeguard themselves from harassment, for which a solution to content moderation is reliant upon. New moderation technologies based on AI work to quarantine harmful content before it is posted on social media platforms, thereby protecting users and manual moderators from viewing such harmful content (Ullmann and Tomalin 2019). This method would strike a balance between free speech and hate speech, shielding users from threats of harassment and general online toxicity.

Policy Recommendations

Based on the digital authoritarian threats outlined in the above case studies, the US government should implement the following policy recommendations to prevent further damage to American democracy:

Recommendation 1

To improve their information security programs, the IRS and the OPM should implement all the GAO's and OPM IG's outstanding recommendations from past information security reports for each respective agency. Additionally, independent oversight agencies should conduct annual audits of federal institutions' information security systems and meaningful consequences must be enforced to ensure federal, political institutions are held accountable for their roles in securing the American democracy from DA forces.

Recommendation 2

It is in America's best interest to restrict its firm's dealings with the Chinese state and its SOEs to limit further legitimization of the China Model alternative. This issue should be addressed both at the state level, and multilaterally through the OECD by ensuring proper redress mechanisms exist against anti-competitive practices, technology transfers are limited or prevented, and intellectual property is protected by enforcing pre-existing standards. The US should also encourage equitable partnerships with emerging democracies to ensure the continued use of its own systems, such as GPS, and to highlight the transparency offered in American leadership.

Recommendation 3

The US Congress needs to halt the use of FRT federally until state-led policies are implemented on its use by law enforcement. These policies must include the regulation of everyday use of FRT by local officers and the instilling of administrative checks and balances in the form of permission requests and time-limits on the use of FRT. Moving forward, Massachusetts' Bill S.2963 presents a tangible example for decision makers on how these policies can be implemented on a state-level and why immediate federal regulatory action is necessary.

Recommendation 4

It is recommended that the US federal government implement fines for technology companies who fail to promptly remove hate speech and violent content, to increase each platform's accountability and ensure they adhere to their regulation policies. Furthermore, the US government should require platforms to report Americans' online violent speech to US authorities when there is a presumed risk of real-world violence, to decrease the number of organized hate crimes.

Recommendation 5

Given the unequal application often accompanying manual content moderation and reliance on user generated flagged content, formulating, and implementing base AI operations that can analyze content before being uploaded is key. The approach of the quarantine method will accomplish this by alerting recipients of harmful content from other users and allowing them to choose whether they would like to view it. To ensure consistent regulation across platforms, federal policy should aim to work alongside platforms in establishing clear AI operations that can be implemented within popular platforms like Facebook and Twitter.

Conclusions

To conclude, this policy report has outlined a variety of democratic vulnerabilities to the rise of DA in the US and proposed several solutions for the American federal government to curb these trends. Given many federal institutions' lax information security measures, they need to be diligent in implementing outstanding information security recommendations from oversight agencies and they should be subject to annual security audits, as well as meaningful consequences for noncompliance. American institutions can no longer bear the brunt of its firm's negligence within the international community, and its corporations must be held to liberal democratic standards in their interactions with authoritarian regimes. Following concerns over the discriminatory and inaccurate nature of FRT and its impact on democratic freedoms, the federal government needs to enact regulations on the arbitrary use of this technology by local law enforcement to ensure legislative checks and balances are implemented concerning how it should be used within investigations. Given the struggles associated with manual content moderation and limitations to freedom of speech within social media platforms, the quarantining method will effectively reduce the gap between acceptable online behaviour and hate speech as it relates to user experience. Because of the US's lax regulations surrounding new technologies that facilitate sharp power and reproduce systems of oppression, failure to act on these current trends of DA will further degrade Americans' trust in democratic values and institutions, thereby harming global democratic standards.

References

67th Congress. 1921. *An Act to Provide a National Budget System and an Independent Audit of Government Accounts, and for Other Purposes*. https://www.gao.gov/assets/D03855.pdf.

105th Congress. 1998. *An Act to Amend the Internal Revenue Code of 1986 to Restructure and Reform the Internal Revenue Service, and for Other Purposes*. https://www.congress.gov/105/plaws/publ206/PLAW-105publ206.pdf.

113th Congress. 2014. *An Act to Amend Title 5, United States Code, to Provide That the Inspector General of the Office of Personnel Management May Use Amounts in the Revolving Fund of the Office to Fund Audits, Investigations, and Oversight Activities, and for Other Purposes.* https://www.congress.gov/113/plaws/publ80/PLAW-113publ80.pdf.

192nd General Court of the Commonwealth of Massachusetts. 2020. *An Act Relative to Justice, Equity and Accountability in Law Enforcement in the Commonwealth*. https://malegislature.gov/Bills/191/S2963?=11302020.

Abrams, Floyd. 2012. "Chapter 6: On American Hate Speech Law." In *The Content and Context of Hate Speech: Rethinking Regulation and Responses*, edited by Michael Herz and Peter Molnar. Cambridge: Cambridge University Press. doi: 10.1017/CBO9781139042871.

Angwin, Julia, and Hannes Grassegger. 2017. "Facebook's Secret Censorship Rules Protect White Men from Hate Speech but Not Black Children." *ProPublica*, June 28, 2017. https://www.propublica.org/article/facebook-hate-speech-censorship-internal-documents-algorithms.

Arpino, Bruno, and Anastassia V. Obydenkova. 2020. "Democracy and Political Trust Before and After the Great Recession 2008: The European Union and the United Nations." *Social Indicators Research* 148 (2): 395–415. doi: 10.1007/s11205-019-02204-x.

Astor, Maggie. 2018. "For Female Candidates, Harassment and Threats Come Every Day." *The New York Times*. August 24, 2018. https://www.nytimes.com/2018/08/24/us/politics/women-harassment-elections.html.

Atsmon, Yuval, Max Magni, Lihua Li, and Wenkan Liao. 2012. "Meet the 2020 Chinese Consumer." McKinsey Consumer & Shopper Insights. McKinsey & Company. https://www.mckinsey.com/~/media/mckinsey/featured%20insights/asia%20pacific/meet%20the%20chinese%20consumer%20of%202020/mckinseyinsightschina%20meetthe2020chineseconsumer.pdf.

Bader, Julia, Jörn Grävingholt, and Antje Kästner. 2010. "Would Autocracies Promote Autocracy? A Political Economy Perspective on Regime-Type Export in Regional Neighbourhoods." *Contemporary Politics* 16 (1): 81–100. doi: 10.1080/13569771003593904.

Ben-David, Anat, and Ariadna Matamoros-Fernández. 2016. “Hate Speech and Covert Discrimination on Social Media: Monitoring the Facebook Pages of Extreme-Right Political Parties in Spain.” *International Journal of Communication* 10 (1): 1167–93. https://ijoc.org/index.php/ijoc/article/view/3697.

Brunk, Jens, Jana Mattern, and Dennis M. Riehle. "Effect of transparency and trust on acceptance of automatic online comment moderation systems." *European Research Center for Information Systems* (2019) pp. 1-7. doi: 10.1109/CBI.2019.00056.

Chen, Jane. 2016. “Cyber Security: Bull’s-Eye on Small Businesses.” *Journal of International Business and Law* 16 (1): 97–118. https://scholarlycommons.law.hofstra.edu/cgi/viewcontent.cgi?article=1309&context=jibl.

Chen, Ming Shin. 2019. “China’s Data Collection on US Citizens: Implications, Risks, and Solutions.” *Journal of Science Policy & Governance* 15 (1): 1–14. https://www.sciencepolicyjournal.org/uploads/5/4/3/4/5434385/chen_jspg_v15.pdf.

Cheney, Clayton. 2019. “China’s Digital Silk Road: Strategic Technological Competition and Exporting Political Illiberalism.” *Issues & Insights. Pacific Forum*. https://www.pacforum.org/analysis/issues-insights-vol-19-wp8-–-chinas-digital-silk-road-strategic-technological-competition.

Crofts, Penny, and Honni van Rijswijk. 2020. “Negotiating ‘Evil’: Google, Project Maven and the Corporate Form.” *Law, Technology and Humans* 2 (1): 5–91. doi: 10.5204/thj.v2il.1313.

Darby, Christopher, and Sarah Sewall. 2021. “The Innovation Wars,” February 18, 2021. https://www.foreignaffairs.com/articles/united-states/2021-02-10/technology-innovation-wars.

Doyle, Jude. 2017. “Trainwreck: The Women We Love to Hate "For the First Time, Death Threats Forced a Woman Out of a Congressional Race. It Won't Be the Last." ELLE. October 11, 2017. https://www.elle.com/culture/career-politics/news/a45762/kim-weaver-iowa-congressional-race-death-threats/.

Duffy, Clare. 2020. “Microsoft’s president calls for federal regulation of facial recognition technology.” CNN. February 27, 2021. link.gale.com/apps/doc/A626972535/AONE?u=ocul_mcmaster&sid=AONE&xid=2bef7753.

Electronic Frontier Foundation. n.d. “Section 230 of the Communications Decency Act.” https://www.eff.org/issues/cda230.

Facebook Community Standards. 2021. "Objectionable Content," 2021. https://www.facebook.com/communitystandards/objectionable_content.

Falsetta, Diana. 2020. "Discussion of Trust and Compliance Effects of Taxpayer Identity Theft: A Moderated Mediation Analysis." *Journal of the American Taxation Association* 42 (1): 79–81. doi: 10.2308/atax-52517.

Freedman, Josh. 2021. "Why Beijing Is Bringing Big Tech to Heel," February 4, 2021. https://www.foreignaffairs.com/articles/china/2021-02-04/why-beijing-bringing-big-tech-heel.

Gallagher, Ryan. 2018. "Google Plans to Launch Censored Search Engine in China, Leaked Documents Reveal." The Intercept. August 1, 2018. https://theintercept.com/2018/08/01/google-china-search-engine-censorship/.

Gallagher, Ryan. 2019. "Google Employees Uncover Ongoing Work on Censored China Search." The Intercept. March 4, 2019. https://theintercept.com/2019/03/04/google-ongoing-project-dragonfly/.

Gangadharan, Seeta Pena. 2021. "Digital Exclusion: A Politics of Refusal." In *Digital Technology and Democratic Theory*, 113-140. Chicago: University of Chicago Press, 2021. http://eprints.lse.ac.uk/id/eprint/103076.

GAO. 2015. "INFORMATION SECURITY: IRS Needs to Continue Improving Controls over Financial and Taxpayer Data." United States Government Accountability Office GAO-15-337. Report to the Commissioner of Internal Revenue. Government Accountability Office. https://www.gao.gov/assets/gao-15-337.pdf.

GAO. 2016. "INFORMATION SECURITY: Agencies Need to Improve Controls over Selected High-Impact Systems." United States Government Accountability Office GAO-16-501. Report to Congressional Requesters. Government Accountability Office. https://www.gao.gov/assets/gao-16-501.pdf.

GAO. 2017. "INFORMATION SECURITY: Control Deficiencies Continue to Limit IRS's Effectiveness in Protecting Sensitive Financial and Taxpayer Data." United States Government Accountability Office GAO-17-395. Report to the Commissioner of Internal Revenue. Government Accountability Office. https://www.gao.gov/assets/gao-17-395.pdf.

GAO. 2018a. "IDENTITY THEFT: IRS Needs to Strengthen Taxpayer Authentication Efforts." United States Government Accountability Office GAO-18-418. Report to Congressional Requesters. Government Accountability Office. https://www.gao.gov/assets/gao-18-418.pdf.

GAO. 2018b. "INFORMATION SECURITY: IRS Needs to Rectify Control Deficiencies That Limit Its Effectiveness in Protecting Sensitive Financial and Taxpayer Date." United States Government Accountability Office GAO-18-391. Report to the Commissioner of

Internal Revenue. Government Accountability Office. https://www.gao.gov/assets/gao-18-391.pdf.

GAO. 2019. “CYBERSECURITY: Agencies Need to Fully Establish Risk Management Programs and Address Challenges.” United States Government Accountability Office GAO-19-384. Report to Congressional Requesters. Government Accountability Office. https://www.gao.gov/assets/gao-19-384.pdf.

GAO. 2021. “What GAO Does.” Government Website. April 7, 2021. https://www.gao.gov/about/what-gao-does.

Garvie, Clare, and Jonathan Frankle. 2016. “Unregulated Police Face Recognition in America.” *Georgetown Law: Center on Privacy & Technology*. October 18, 2016. https://www.perpetuallineup.org/.

Ghosh, Dipayan. 2020. “It’s All in the Business Model: The Internet’s Economic Logic and the Instigation of Disinformation, Hate, and Discrimination.” *Georgetown Journal of International Affairs* 21 (1): 129–35. doi: 10.1353/gia.2020.0012.

Goodwin, Blaine. 2019. "Regulating Twitter as a Public Utility to Ensure Nondiscrimination." *Cumberland Law Review* 50 (2): 597-638. https://heinonline.org/HOL/P?h=hein.journals/cumlr50&i=609.

Gootman, Stephanie. 2016. “OPM Hack: The Most Dangerous Threat to the Federal Government Today.” *Journal of Applied Security Research* 11 (4): 517–25. doi: 10.1080/19361610.2016.1211876.

Goswami, Namrata. 2020. “The Economic and Military Impact of China’s BeiDou Navigation System.” July 1, 2020. https://thediplomat.com/2020/07/the-economic-and-military-impact-of-chinas-beidou-navigation-system/.

Gravett, Willem. 2020. “Digital Neo-Colonialism: The Chinese Model of Internet Sovereignty in Africa.” *African Human Rights Law Journal* 20 (1): 125–46. doi: 10.17159/1996-2096/2020/v20n1a5.

Grygiel, Jennifer, and Nina Brown. 2019. “Are Social Media Companies Motivated to Be Good Corporate Citizens? Examination of the Connection between Corporate Social Responsibility and Social Media Safety.” *Telecommunications Policy* 43 (5): 445–60. doi: 10.1016/j.telpol.2018.12.003.

Guynn, Jessica. 2019. “Facebook While Black: Users Call It Getting ‘Zucked,’ Say Talking about Racism Is Censored as Hate Speech.” *USA Today*, April 24, 2019. https://www.usatoday.com/story/news/2019/04/24/facebook-while-black-zucked-users-say-they-get-blocked-racism-discussion/2859593002/.

Haines, Errin. 2021. "Rep. Ayanna Pressley: 'What Do You Do When Your Very Existence Is Resistance?'" *USA Today*. January 03, 2021. Accessed April 02, 2021. https://www.usatoday.com/story/news/politics/2021/01/03/threats-squad-member-ayanna-pressley-stands-ground/4093584001/.

Hemmings, John. 2020. “Reconstructing Order: The Geopolitical Risks in China’s Digital Silk Road.” *Asia Policy* 27 (1): 5–21. doi: 10.1353/asp.2020.0002.

Henschke, Adam, Matthew Sussex, and Courteney O’Connor. 2020. “Countering Foreign Interference: Election Integrity Lessons for Liberal Democracies.” *Journal of Cyber Policy* 5 (2): 180–98. doi: 10.1080/23738871.2020.1797136.

Hern, Alex. 2021. “Human rights groups urge New York to ban police use of facial recognition.” *The Guardian*, January 26, 2021. link.gale.com/apps/doc/A649680197/AONE?u=ocul_mcmaster&sid=AONE&xid=3eef8957.

Hill, Kashmir. 2021. “How One State Manages to Actually Write Rules on Facial Recognition” *The New York Times*, February 27, 2021. https://www.nytimes.com/2021/02/27/technology/Massachusetts-facial-recognition-rules.html.

Hill, Kashmir. 2021. “The Secretive Company That Might End Privacy as We Know It.” *The New York Times*, January 18, 2021. https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

Huffpost. 2015. “IRS Data Breach Shows Why the Government Needs to Modernize Its Online Security, Now.” *Huffpost*, June 3, 2015. https://www.huffpost.com/entry/irs-data-breach_n_7503874.

IRS. 2016. “IRS Statement On ‘Get Transcript.’” Government Website. Internal Revenue Service. February 26, 2016. https://www.irs.gov/newsroom/irs-statement-on-get-transcript.

IRS. 2020a. “The Agency, Its Mission and Statutory Authority.” Government Website. Internal Revenue Service. September 28, 2020. https://www.irs.gov/about-irs/the-agency-its-mission-and-statutory-authority.

IRS. 2020b. “IRS Oversight Organizations.” Government Website. Internal Revenue Service. December 17, 2020. https://www.irs.gov/about-irs/irs-oversight-organizations.

Jackson, Christopher et al. 2020. “Establishing Privacy Advisory Commissions for the Regulation of Facial Recognition Systems as the Municipal Level.” *University of California Berkeley eScholarship*: 1-7. https://escholarship.org/uc/item/7qp0w9rn.

Johnson, Corey. 2021. “A Local Law to amend the administrative code of the city of New York, in relation to creating comprehensive reporting and oversight of New York city police department surveillance technologies.” *The New York City Council*, February 18, 2021. https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=3343878&GUID=996ABB2A-9F4C-4A32-B081-D6F24AB954A0.

Kadri, T. E., and Kate Klonick. 2019. “Facebook v. Sullivan: Public Figures and Newsworthiness in Online Speech.” *Southern California Law Review* 93 (1): 37-[x]. https://scholarship.law.stjohns.edu/cgi/viewcontent.cgi?article=1292&context=faculty_publications.

Kato, Junko, and Seiki Tanaka. 2019. “Does Taxation Lose Its Role in Contemporary Democratisation? State Revenue Production Revisited in the Third Wave of Democratisation.” *European Journal of Political Research* 58 (1): 184–208. doi: 10.1111/1475-6765.12276.

Kerr, Jaclyn. 2018. “The Russian Model of Digital Control and Its Significance.” In *AI, China, Russia, and the Global Order: Technological, Political, Global, and Creative Perspectives*, by Benjamin Angel Chang, Rogier Creemers, Regina Joseph, James A Lewis, Martin Libicki, Herbert Lin, Kacie Miura et al., 55–72. United States Department of Defense. https://apps.dtic.mil/sti/pdfs/AD1066673.pdf.

Klare, Brendan F. et al. 2012. “Face Recognition Performance: Role of Demographic Information.” *IEEE Transactions on Information Forensics and Security*: 1-14. doi: 10.1109/TIFS.2012.2214212.

Klonick, Kate. 2020. “The Facebook Oversight Board: Creating an Independent Institution to Adjudicate Online Free Expression.” *The Yale Law Journal* 129 (1): 2418–99. https://ssrn.com/abstract=3639234.

Krook, Mona Lena, and Juliana Restrepo Sanín. 2020. "The cost of doing politics? Analyzing violence and harassment against female politicians." *Perspectives on Politics* 18 (3): 740-755. doi: 10.1017/S1537592719001397.

Leslie, David. 2020. “Understanding bias in facial recognition technologies: an explainer”. *The Alan Turing Institute*. doi: 10.5281/zendodo.4050457.

Levy, Pema. 2020. “Black Activists Warn That Facebook Hasn’t Done Enough to Stop Racist Harassment.” *Mother Jones*, July 9, 2020. https://www.motherjones.com/politics/2020/07/facebook-black-lives-matter/.

Liu, Lizhi. 2021. “The Rise of Data Politics: Digital China and the World.” *Studies in Comparative International Development* (56) March, 19: 45-67. doi: 10.2139/ssrn.3669452.

Lührmann, Anna, and Staffan I. Lindberg. 2019. “A Third Wave of Autocratization Is Here: What Is New About It?” *Democratization* 26 (7): 1095–1113. doi: 10.1080/13510347.2019.1582029.

Markey, Ed. 2020. “Senators Markey and Merkley, and Reps. Jayapal, Pressley to Introduce Legislation to Ban Government Use of Facial Recognition, Other Biometric Technology.” *Ed Markey News.* June 25, 2020. https://www.markey.senate.gov/news/press-releases/senators-markey-and-merkley-and-reps-jayapal-pressley-to-introduce-legislation-to-ban-government-use-of-facial-recognition-other-biometric-technology.

Marshak, Emma. 2017. "Online harassment: A legislative solution." *Harv. J. on Legis.* 54: 503-34. https://heinonline.org/HOL/P?h=hein.journals/hjl54&i=511.

Matthews, Kyle, and George Tsagaroulis. 2020. “Why Canada Must Confront the Rise of Digital Authoritarianism.” *Open Canada*. November 18, 2020. https://opencanada.org/why-canada-must-confront-the-rise-of-digital-authoritarianism/.

Mekouar, Dora. 2019. "For Women in Politics, Being Terrorized Comes with the Job." *Voice of America*. August 23, 2019. https://www.voanews.com/usa/all-about-america/women-politics-being-terrorized-comes-job.

Michaelsen, Marcus, and Marlies Glasius. 2018. “Authoritarian Practices in the Digital Age.” *International Journal of Communication 12*: 3788-3794. doi: 1932–8036/20180005.

Morgan, Steve. 2016. “IRS Reports 700,000 U.S. Taxpayers Hacked And 47 Million ‘Get Transcripts’ Ordered.” *Forbes*, February 28, 2016, sec. Tech. https://www.forbes.com/sites/stevemorgan/2016/02/28/irs-reports-700000-u-s-taxpayers-hacked-and-47-million-get-transcripts-ordered/.

National Museum of African History and Culture. 2019. “Social Identities and Systems of Oppression.” *National Museum of African History and Culture.* 2021. https://nmaahc.si.edu/learn/talking-about-race/topics/social-identities-and-systems-oppression.

National Security Agency. 2021. “Understanding the Threat.” Government Website. *National Security Agency*. 2021. https://www.nsa.gov/what-we-do/understanding-the-threat/.

Nesterova, Irena. 2019. “Mass data gathering and surveillance: the fight against facial recognition technology in the globalized world.” *SHS Web Conferences 74*: 1-8. doi: 10.1051/shsconf/2020743006.

Neubert, Mitchell J., and George D. Montañez. 2020. “Virtue as a Framework for the Design and Use of Artificial Intelligence.” *Business Horizons*, ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING, 63 (2): 195–204. doi: 10.1016/j.bushor.2019.11.001.

Newman, Lily Hay. 2019. “Facial Recognition Has Already Its Breaking Point.” *Wired*, May 22, 2019. https://www.wired.com/story/facial-recognition-regulation/.

New York Post. 2015. “IRS Hack Came from Russia.” *New York Post*, May 27, 2015. https://nypost.com/2015/05/27/irs-hack-came-from-russia/.

Nurik, Chloé. 2019. “‘Men Are Scum’: Self-Regulation, Hate Speech, and Gender-Based Censorship on Facebook.” *International Journal of Communication* 13 (1): 2878–98. https://ijoc.org/index.php/ijoc/article/view/9608/2697.

Nye, Joseph S. 1990. “Soft Power.” *Foreign Policy* (80): 153–71. doi: 10.2307/1148580.

Omand, David. 2018. “The Threats from Modern Digital Subversion and Sedition.” *Journal of Cyber Policy* 3 (1): 5–23. doi: 10.1080/23738871.2018.1448097.

OPM. 2021. “Our Agency.” OPM.gov. U.S. Office of Personnel Management. April 7, 2021. https://www.opm.gov/about-us/.

OPM IG. 2018. “Open Recommendations Over Six Months Old as of September 30, 2018.” U.S. Office of Personnel Management Office of the Inspector General. Office of Personnel Management. https://www.opm.gov/our-inspector-general/publications/open-recommendations/open-recommendations-over-six-months-old-as-of-september-30-2018.pdf.

Polyakova, Alina and Chris Meserole. 2020. “Exporting Digital Authoritarianism: The Russian and Chinese Models.” *Brookings Institution*. https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf.

Rector, Kevin. 2021. “LAPD panel approves new oversight of facial recognition, rejects calls to end program.” *The Los Angeles Times*, January 12, 2021. https://www.latimes.com/california/story/2021-01-12/lapd-panel-approves-new-oversight-of-facial-recognition-rejects-calls-to-end-program.

Reisinger, Don. 2015. “Russian Hackers Behind $50 Million IRS Scheme, Report Says.” *CNET*. May 29, 2015. https://www.cnet.com/news/russian-hackers-behind-50-million-irs-hack-report-says/.

Rice, A.J. 2020. “What Gets You ‘Zucked’ By an Increasingly Woke Facebook.” *Real Clear Markets*, December 17, 2020. https://www.realclearmarkets.com/articles/2020/12/17/what_gets_you_zucked_by_an_increasingly_woke_facebook_653586.html.

Rid, Thomas, and Ben Buchanan. 2018. “Hacking Democracy.” *The SAIS Review of International Affairs* 38 (1): 3–16. doi: 10.1353/sais.2018.0001.

Ringrose, Katelyn. 2019. “Law Enforcement’s Pairing of Facial Recognition Technology with Body-Worn Cameras Escalates Privacy Concerns.” *Virginia Law Review* 105: 57-66. https://www.virginialawreview.org/wp-content/uploads/2020/12/04.%20Final%20Ringrose.pdf.

Roberts, Sarah T. 2019. *Behind the Screen: Content Moderation in the Shadows of Social Media*. New Haven: Yale University Press. doi: 10.2307/j.ctvhrcz0v.

Rosenberger, Laura. 2020. “Making Cyberspace Safe for Democracy,” *Foreign Affairs,* 2020. https://www.foreignaffairs.com/articles/china/2020-04-13/making-cyberspace-safe-democracy.

Saresma, Tuija, Sanna Karkulehto, and Piia Varis. 2021. "Gendered Violence Online: Hate Speech as an Intersection of Misogyny and Racism." In *Violence, Gender and Affect*: 221-243. Palgrave Macmillan, Cham, 2021. doi: 10.1007/978-3-030-56930-3_11.

Schaake, Marietje. 2020. “The Lawless Realm.” *Foreign Affairs*, October 19, 2020. https://www.foreignaffairs.com/articles/world/2020-10-13/lawless-realm.

Schmidt, Eric, Robert Work, Sarah Catz, Steve Chien, Mignon Clyburn, Christopher Darby, Kenneth Ford, et al. 2019. “Interim Report.” *National Security Commission on Artificial Intelligence*. https://www.nationaldefensemagazine.org/-/media/sites/magazine/03_linkedfiles/nscai-interim-report-for-congress.ashx?la=en.

Scott, Mark, and Janosch Delcker. 2019. “Germany Lays down Marker for Online Hate Speech Laws.” *Politico*, October 30, 2019. https://www.politico.eu/article/germany-hate-speech-netzdg-angela-merkel-facebook-germany-twitter/.

Shen, Hong. 2018. “Building a Digital Silk Road? Situating the Internet in China’s Belt and Road Initiative.” *International Journal of Communication* 12: 2683–2701. https://ijoc.org/index.php/ijoc/article/view/8405/2386.

Sherman, Justin. 2021. “Digital Authoritarianism and Implications for US National Security.” *The Cyber Defense Review* 6 (1): 107–18. https://www.jstor.org/stable/26994115.

Silverman, Craig. 2020. “Black Lives Matter Activists Say They’re Being Silenced by Facebook.” *Buzzfeed News*, June 19, 2020. https://www.buzzfeednews.com/article/craigsilverman/facebook-silencing-black-lives-matter-activists.

Silverman, Jacob. 2017. “Privacy Under Surveillance Capitalism.” *Social Research: An International Quarterly* 84 (1): 147-164. https://muse.jhu.edu/article/659227/pdf.

Siripurapu, Anshu, and William Merrow. 2021. “Social Media and Online Speech: How Should Countries Regulate Tech Giants?” *Council on Foreign Relations,* February 9, 2021.

https://www.cfr.org/in-brief/social-media-and-online-speech-how-should-countries-regulate-tech-giants.

Smart Policing Initiative. 2017. *Smart Policing Initiative: Data, Analysis, Solutions*. U.S. Bureau of Justice Assistance. https://bja.ojp.gov/sites/g/files/xyckuh186/files/Publications/SmartPolicingFS.pdf.

O'Sullivan, Donie. "Twitter Bans Posts Wishing for Trump Death. The Squad Wonders Where That Policy Was for Them." *CNN*. October 03, 2020. https://www.cnn.com/2020/10/03/politics/twitter-trump-policy-ban-the-squad-politics-trnd/index.html.

Sunstein, Cass R. 2017. "Chapter 1: The Daily Me." In *#Republic: Divided Democracy in the Age of Social Media*, 16–45. doi: 10.1515/9781400884711.

Tan, Netina. 2021. "Digital Authoritarianism." Lecture, McMaster University, Hamilton, ON, January 27, 2021. Accessed April 1, 2021.

TIGTA. 2020. "U.S. Treasury Inspector General for Tax Administration (TIGTA)." Government Website. Treasury Inspector General for Tax Administration (TIGTA). December 3, 2020. https://www.treasury.gov/tigta/.

Ullmann, Stefanie, and Marcus Tomalin. 2020. "Quarantining online hate speech: technical and ethical perspectives." *Ethics and Information Technology* 22 (1): 69-80. doi: 10.1007/s10676-019-09516-z

Vail, Hannah. 2017. "Cybersecurity Reform in the Wake of the OPM Breach Notes." *Suffolk University Law Review* 50 (1): 221–36. https://cpb-us-e1.wpmucdn.com/sites.suffolk.edu/dist/3/1172/files/2017/04/Vail_Note_FR-2.15.pdf.

Valentino-DeVries, Jennifer. 2020. "How the Police Use Facial Recognition, and Where It Falls Short." *The New York Times*, June 12, 2020. https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html.

van der Meer, Tom W. G. 2017. "Political Trust and the 'Crisis of Democracy.'" *Oxford Research Encyclopedia of Politics*, January, 1–21. doi: 10.1093/acrefore/9780190228637.013.77.

Walker, Christopher, and Jessica Ludwig. 2017. "From 'Soft Power' to 'Sharp Power': Rising Authoritarian Influence in the Democratic World." In *Sharp Power: Rising Authoritarian Influence*, by Juan Pablo Cardenal, Jacek Kucharczyk, Grigorij Mesežnikov, and Gabriela Pleschová. National Endowment for Democracy. https://www.ned.org/wp-content/uploads/2017/12/Sharp-Power-Rising-Authoritarian-Influence-Full-Report.pdf.

Weiss, Jessica Chen. 2019. “A World Safe for Autocracy? China’s Rise and the Future of Global Politics.” *Foreign Affairs,* August 2019. https://www.foreignaffairs.com/articles/china/2019-06-11/world-safe-autocracy.

Woo, Ryan, and Liangping Gao. 2020. “China Set to Complete Beidou Network Rivalling GPS in Global Navigation.” *Reuters,* June 11, 2020. https://www.reuters.com/article/us-space-exploration-china-satellite-idUSKBN23J0I9.

Yayboke, Erol, and Sam Brannen. 2020. “Promote and Build: A Strategic Approach to Digital Authoritarianism.” *CSIS Briefs,* October 2020: 1-11. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/201015_Yayboke_Brannen_PromoteAndBuild_Brief.pdf.

Zheng, Yanfeng, and Qinyu (Ryan) Wang. 2020. “Shadow of the Great Firewall: The Impact of Google Blockade on Innovation in China.” *Strategic Management Journal* 41 (12): 2234–60. doi: 10.1002/smj.3179.

Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism*. New York, NY: Public Affairs.