

2018

Why Study the Internet?

Joe Fitzgerald
Bard College

Recommended Citation

Fitzgerald, Joe, "Why Study the Internet?" (2018). *Senior Projects Fall 2018*. 25.
https://digitalcommons.bard.edu/senproj_f2018/25

This Open Access is brought to you for free and open access by the Bard Undergraduate Senior Projects at Bard Digital Commons. It has been accepted for inclusion in Senior Projects Fall 2018 by an authorized administrator of Bard Digital Commons. For more information, please contact digitalcommons@bard.edu.

Why Study the Internet?

Senior Project Submitted to
The Division of Social Studies
of Bard College

by
Joe Fitzgerald

Annandale-on-Hudson, New York

December 2018

Acknowledgements

This essay would not have been possible without the help of Tom Keenan, who provided crucial feedback in the years leading up to and during my work on this project. Tom generously agreed to an unusual arrangement for its completion, and while I tried to thank him for his time with coffee, I estimate that this only covered about 75% of what he would have made on the clock at Bard. I thank Tom for the keen alternative perspectives, honest criticism and encouragement he shared along the way to help me develop an idea into a product, and I leave it to up him to set an interest rate on future coffees.

With clear visions of the institution and keen eyes for my academic strengths, weaknesses, and incompatibilities, Annie Seaton and Éric Trudel have been friends, mentors and role models almost since I arrived at Bard. It is difficult to imagine where I would be now without these anchors. Peter Rosenblum and Marina Van Zuylen challenged me to write with purpose, but not without modesty — a crucial skill I have yet to master — and taught me the power of convention. Roger Berkowitz and Tabetha Ewing supported my ambition while serving a crucial dose of reality at times; they taught me first principles of research and argumentation.

In high school, my mother read nearly all of my essays before I submitted them, and the trend continued briefly after I started at Bard. Although she has not yet seen this project, it remains the result of many years of thoughtful feedback and loving encouragement for which I am eternally grateful. My grandfather also supported this project by providing room and board for the final months of writing, a gift and a greater sacrifice perhaps than he would be willing to admit, considering my sleeping habits and how often I forget to entirely close the kitchen drawers.

Fellow students in the human rights department inspired me to work with discipline and rigor, and for these admirable standards I am grateful. But this project was even more heavily inspired by the work of my peers outside the classroom: from student art magazines, journals and newspapers to performances, events, community activism groups and dinner, I found hope and belonging in pockets of passionate and determined students who gave me real-world standards to aspire to in evaluating the integrity of my own work.

Table of Contents

Foreword: About the Project 3

Chapter 1: New Tools for Democratization 5

Chapter 2: Moralizing Internet Governance Theory 32

Chapter 3: Private Industry, Public Square 63

Chapter 4: The Internet and the Ideological State Apparatus 96

Bibliography 108

“Men think about the new in terms of the old: to questions about what the future holds they bring an imagination indoctrinated and colored by the past. This is a terrible way of forming opinions, because streams fed by nature’s springs don’t run along familiar channels.”

–Francis Bacon, *Novum Organum* (1620)

Foreword: About the Project

I pinpoint the origins of this project around three years ago, when I discovered an archive of hundreds of student newspapers and publications at Bard spanning back to 1895. In 1999 two Seniors at Bard, Nate Schwartz and Joe Stanco, scanned and annotated digital copies of thousands of pages stored in the College's student newspaper archive, with help from faculty and students in the Computer Science Department, the History Department, and the archival office.¹ Poring through the archive in 2016, I reveled in the passion with which countless Bard students once pursued local community journalism. But in dismay, I saw the absence of any serious student newspapers at Bard today and wondered, where had all that passion gone?

After a number of failed attempts to help student publications to transition to digital-first models, in light of the death of the newspaper at Bard and the evolving news consumption habits of my peers, I was forced to step back from the frontline to focus on my graduation requirements (i.e. this project). Despite my initial reluctance to spend what I thought would be wasted time behind a keyboard, I quickly discovered the value in the opportunity to reflect deeply on what I have been studying in and outside of the classroom at Bard. As a natural consequence of my moderating into the Human Rights Department, this project is primarily rooted in associated vocabularies and concepts. But considering my extracurricular work with newspapers and my personal interests in sociology and digital technologies, the true object of this essay is the Internet, and the implications of our different relationships to the technology for new images of society and self. If it does nothing else for you, I hope this essay at least prompts you to more seriously consider deleting your Facebook account.

¹ <http://www.bard.edu/library/archive/newspapers/guide/credits.html>

Chapter 1: New Tools for Democratization

During Barack Obama's first run for president, fewer than 10 percent of Americans used social media.¹ Yet he and his advisors acutely recognized the potential for a new kind of "networked, open-source campaign" unlike any before, as the *New York Times* called it the day after his nomination.² In 2008, the Illinois Senator boasted 2 million supporters on Facebook, compared to 600,000 for John McCain. On Twitter, McCain's 4,600 followers stood little chance against Obama's 112,000 supporters, and the BarackObama.com YouTube channel accumulated close to 100 million views, nearly four times that of his Republican competitor.³ On election day, two-thirds of voters under 30 backed the democratic candidate, making the disparity between younger voters and other age groups greater in 2008 than in any other presidential election since 1972. The link between Obama's digital presence and the youth vote was immediately clear.⁴ In a conversation with Arianna Huffington on the implications of the 2008 election, one commentator remarked: "This medium demands authenticity, and television for the most part demanded fake. Authenticity is something politicians haven't been used to."⁵

Others were slower to realize the implications of the new medium for influencing public opinion. In 2008 for instance Republican candidates mostly failed to incorporate social networking tactics into their campaigns. Allison Slotnick pointed out that even in 2009, "Rudy Giuliani, not surprisingly, 'doesn't exist on Facebook.'"⁶ In her essay, Slotnick highlighted the shifting landscape for public discourse and political campaigning, arguing that "virtual communities" formed online and on social media are making traditional organizing tactics obsolete. The author explained: "local and personal relationship building has been largely

replaced by a global network of individuals who in many cases will never actually meet face to face.”⁷ Slotnick thus joined a growing body of scholarship conceptualizing new informations and communications technologies (ICTs) in terms of a “global network of individuals” that political campaigns and other public influence operations can employ for advancing their goals.

The “network society,”⁸ a concept sociologist Manuel Castells popularized in the late 1990s, depicts a world of individuals linked through interconnected networks of platforms for communicating and sharing information, representing a key manifestation of what the Italian philosopher Luciano Floridi calls our “Information Age.”⁹ Utopian visions for the network society based on social media in particular have gained significant traction over the past decade, especially in the aftermath of Barack Obama’s successive nominations and a series of popular uprisings known as the “Arab Spring” that relied heavily on digital social networking tools. But as digital networking technologies have opened new corners of the globe to powerful tools for organization, democratization and freedom of expression, the same systems have also cultivated a complex web of censorship and manipulation programs reaching equally distant and diverse regions. Rapid technological advancements and ICT proliferation since the early 1990s have corresponded with a paradigm shift in human rights theory, as scholars strive to adapt a cohesive version of a traditionally regional discourse to remain relevant in an increasingly globalized world. I will explore the notion of ‘globalization’ at greater length in Chapter 2, but for now it is sufficient merely to acknowledge that the Internet represents a uniquely international phenomenon not just among other ICTs but as a crucial underlying force behind changes in the concept of the “international” over the past three decades in mainstream theory.

The profound and dual-edged impacts of the Internet on human rights and free speech work in fact embody even broader tensions in contemporary theories on society and on being. In the effort to update a historical discipline to tackle postmodern theories of globalism and society, human traditional rights scholars tend to hit a discursive wall where the universal subject meets a multicultural value system. In 2016, Wendy Hui Kyong Chun illustrated how the material reality of the Information Age aggravates these growing internal contradictions, stating simply:

“Networks end postmodernism.” Chun expanded:

They counter the pastiche with the zoom and the overview, they animate and locate ‘wherever’ architecture; they resolve multiculturalism through neighborhood predictors that bypass yet reinforce categories such as race, gender, sexuality; they replace postmodern relativism with data analytics.¹⁰

Human rights discourse in this context provides an ideal entry point for examining fundamental shifts in modern psychology related to the emergence of the network society, as mainstream rights scholars struggling to reconcile universalism with a global technology undertake an endeavor similar to that of how Chun describes networks replacing postmodernism. Whereas traditional human rights theorists actively seek to “resolve multiculturalism” by fortifying a universal vision of the subject of rights in order to equalize all members of our species under an equivalent moral umbrella, networks filter passively in the opposite direction by atomizing subjects under various categories of identity posited in postmodern thought.

Human rights scholars today often see networks primarily as tools for advancing conventional rights work. But networks also play an active role in shaping the discourse itself, in many cases both comprising the infrastructural landscape and determining the possible forms of

intervention for human rights workers concerned with rights related to ICTs and the Internet.

Chun elaborated on networks, writing: “They imagine connections that transform the basis of the collective imaginary from ‘we’ to YOU: from community to an ever-resolvable grouping that erodes and sustains the distance between the self and the other.”¹¹ Chun’s language here echoes the intense focus on the individual inherent to social media platforms, wherein users are asked to create digital versions of themselves to represent a personalized public presence in the network society. Social media platforms thus replicate the paradoxical processes of both universalization and atomization simultaneously, similar to how networks and human rights discourse respectively dismantle postmodern distinctions, by presenting users with standardized formats and vocabularies to use in establishing their public digital identities.

My goal in researching and writing this project was to better understand the relationship between social media, the Internet and human rights discourse. My secondary goal was to target the very limited audience of this work more directly — my professors — both to demonstrate my grasp of the topic at hand and to urge them to more seriously heed the weight of the impacts of the Internet on the human rights discipline than I sense is common among members of generations older than my own. To this end, in the following chapters I explore the historical interplay between emerging technologies moral theories, focusing in particular on how mainstream human rights theorists have responded and adapted to the increasing power of the private sector in issues related to Internet governance. These analyses illustrate the emergence of a profound compatibility between the international human rights regime and social media companies with immense power over shaping freedom of speech and public discourse. The middle chapters of the project exhibit my true feelings about previous work submitted to the

Department by appending additional analyses to an otherwise relatively narrow exploration of theories and concepts related to human rights and the Internet. In the fourth and final chapter, I discuss some of the broader sociological and psychological implications of the Internet through an Althusserian lens, exploring how private industry power works in tandem with state repression to stabilize public discourse on new dominant modes of production in the Information Age. Transposing Althusser's model of the Ideological State Apparatus onto contemporary discussions about social media can help illuminate the invisible consequences of novel forms of censorship and information manipulation in the digital age. But I am getting ahead of myself.

Chapter 1 sets the scene: optimistic visions for the democratizing effects of the Internet abound, popular accounts of the relationship between the Internet, democracy and human rights in the late 2000s and early 2010s epitomized a period of hopefulness. Return to the 2008 Presidential election: comparing the Democratic frontrunners' Facebook profiles with those of the Republican frontrunners, Allison Slotnick's analysis exhibited growing optimism on the left surrounding the Internet's potentially democratizing effects on society. She explained, "the hope is that the key to producing an engaged electorate lies in opening the door at an early age and communicating through a familiar medium," suggesting future interest in capitalizing on the power of new technologies to connect with voters.¹² Obama's victory — the result of what many observers proudly called "The Facebook Election" — hinted at a new political era.^{13 14 15}

Facebook's global user base doubled in size during Obama's first term, growing to over a billion monthly active accounts by the following election cycle. With a three-year head start on the platform, the incumbent again dominated the "Facebook Campaign Wars" — in June 2012, Mitt Romney had acquired 2 million Facebook likes, in contrast to 27 million for Obama.¹⁶ This

time the digital platform also provided significantly more advanced tools for campaigns to use to connect with voters in 2012 than in the previous election. In August, the “Politics & Government Team” at Facebook announced that 1 million apps and websites had “integrated with Facebook,” in a blog post titled: “Facebook Apps Bring the Power of Friends to the Political Process.” The post described an online space heavily saturated by political content generated by Facebook users and collected by the company’s partners, three months before the election: “Some are saying that the 2012 election cycle is already the most ‘social’ in history,” read the post. “We think the developers above are helping to drive this movement by bringing the power of friends to the political process.”¹⁷ Here Facebook’s Politics and Government team demonstrated perhaps the most common trend within the private sector regarding the link between social media, politics and society: self-congratulations.

Journalists mostly echoed Facebook’s optimism. For instance, *The Washington Post* reflected after the 2012 election, “Once is an anomaly. Twice is a new political reality.”¹⁸ Others specifically credited the Obama campaign’s novel application of data accumulated through social networks with ushering in this reality.¹⁹ By integrating its volunteer sign-up app with a Facebook feature called “Connected Apps,” the democratic party had gained access to the ages, postal addresses, occupations and voting histories of millions of American voters “by asking their friends to register to vote, give money, vote or look at a video designed to change their mind.” The feature depended on a vast network of interconnected users — giving the Obama campaign access to the data of 600,000 key supporters and their “friends” — including age, postal address, occupation and voting history.²⁰ Up to 5 million Facebook users in key voting districts, selected using data acquired through Facebook, received a message, invitation, or other interaction from

“friends” who had signed into the Obama campaign app using Facebook and were prompted to “share” or “like” a related message or post. Keen observers settled on a new and perhaps more accurate moniker this time around, calling 2012 “the data election.”²¹

Speculation about the future of political elections accompanied optimism among scholars following Obama’s renomination, although some commentators responded with more cautious awareness of the unpredictable nature of the new medium’s long-term impact. As Michael Scherer argued in *Time*, Obama’s second election had only scratched the surface of the potential applications of Internet and networking technologies in political campaigns: “In 2008, Twitter was a sideshow and Facebook had about one-sixth its current reach in the U.S. By 2016, this sort of campaign-driven sharing over social networks is almost certain to be the norm. Tell your friends.”²² Scherer acutely forecasted the normalization of social networking and online political campaigns over the coming years. Obama’s nomination —and his campaign’s expert use of data from social media companies to target voters — mostly excited political pundits and human rights scholars alike, who held high hopes for the Internet’s impact on liberal agendas.²³ With another more sober outlook resembling that of Michael Scherer, Sarah Green Carmichael, editor at *Harvard Business Review*, advised after Obama’s second victory that the Internet introduces new challenges and demands, in addition to its potential advantages:

What’s interesting to me is that the volumes of data are exploding terribly quickly. The toolkit is also expanding by leaps and bounds. This is a real new arms race. You might not love it, and you might wish the world was predictable and calm and that Excel would get you through — but that would be a recipe for disaster.²⁴

Carmichael suggested that political campaign advisors, journalists and pundits would need to imagine new methods for exploiting these fast growing technologies, rather than relying on familiar tools, to keep up with advances in data-parsing algorithms and programs built to collect personal information. Journalists like Carmichael and Scherer embodied a mentality sweeping not just the media, but through the minds of politicians and voters as well — a cautiously optimistic expectation for the revolution in information and communication technologies to fortify democratic and liberal ideals, perhaps globally. Read one particularly ironic headline from an online news site in February 2012: “Team Obama eyes FB as trump card.”²⁵

The Obama success story on social media serves as a poignant starting place for this project because the example demonstrates the susceptibility of public discourse to major rapid shifts in narratives about how novel technologies impact different political forces in society. Neither am I immune from this form of reactionism, as may become clear by the end of this essay. But the concept will be important to keep in mind as I shift to talking about more apparently negative consequences of the Internet later, for recalling the volatility of perceptions of particular technologies in different communities under different circumstances in my experience is key to preserving any semblance of hope for the future.

Cautious optimism regarding the intersection between social media platforms and democracy in the United States following Obama’s successive victories online and on the ballots compounded with a growing body of literature celebrating the impacts Facebook, Twitter, Youtube and other social media platforms had had on popular uprisings in Muslim countries in the Middle East and North Africa beginning around 2010. Known collectively as the “Arab

Spring,” a series of revolutions in Tunisia, Egypt, Iran and dozens of other countries manifested largely on digital platforms and employed social network–based organizing strategies. In 2011, theorist Michael Doran named the most optimistic accounts of the Arab Spring after Wael Ghonim, a Google marketing executive who is often credited with starting the revolution in Egypt through posts on Facebook.²⁶ The “Ghonim thesis,” as Doran calls it, posits the Internet as a crucial catalyst for democratization in the 21st century. In an interview, Ghonim stated:

This revolution started online. This revolution started on Facebook. This revolution started in June 2010 when hundreds of thousands of Egyptians started collaborating content. We would post a video on Facebook. It would be shared by 50,000 people on their walls within a few hours. I always said that if you want to liberate a society just give them the Internet. If you want to have a free society, just give them the Internet.²⁷

This theory of the Internet, Doran explains, not only attributes the Arab Spring to social media, but also suggests that the Internet represents a democratizing force in politics and society more broadly. The notion that the technology itself is inherently connected to collective acts of liberation is admittedly tempting. The mere fact that I possess access to a seemingly infinite pool of information and media *feels* freeing. And versions of the “Ghonim thesis” indeed surface frequently in contemporary scholarship, especially as Duran pointed out, following the Arab Spring.

Other readings of the Arab Spring acknowledged the catalytic power of social media, but also zoom out to consider the broader contextual features of particular societies preceding the revolutions, in addition crediting specific technological tools. For example, In *The Dawn of the*

Arab Uprisings: End of an Old Order?, Walter Armbrust offers an alternative explanation for the confluence of revolutions, citing economic pressures on the middle class in a failing neoliberal system as the primary cause for the uprisings. Armbrust suggests that as government leaders have benefited from neoliberal trends towards privatizing essential services, popular revolts embody a reaction against “the erosion of a sense that some human spheres should be outside the logic of markets.”²⁸ The materialization of these reactions in the Arab Spring, according to Armbrust, testified to the power of social networking in enabling collective uprisings against repressive systems. But the author’s more expansive framing of the economic and social contexts for these uprisings also points to the truism that government corruption and abuse of power must precede revolution. In contrast to the relatively singular focus on the Internet characteristic of the Ghonim thesis, Armbrust credits social media platforms for enabling revolutions stemming from deeper issues in society. Armbrust’s approach thus essentializes the impact of technology on social movements, insofar as his model could apply equally to various information and communications technologies (ICTs) other than the Internet, such as radio and television.

An even stronger argument can be made against the Ghonim thesis of the Internet’s implications for democracy by turning back to consider the role new technologies have played in revolutions throughout history, from before the proliferation of digital social networks. The Ghonim thesis crucially asserts that the Internet represents a unique force for democratization, but one need not look back more than half a century to see how other forms of technology have served similar roles in popular uprisings. In *A Dying Colonialism*, Frantz Fanon detailed how a shift in popular perspectives on radio among revolutionaries in Algeria in the 1950s and early 60s enabled members of the liberation movement to transform a tool of colonialism into a

weapon of the revolution. Whereas to many, the radio long stood as a symbol of the oppressor in the country — due to France’s extensive use of the medium for reporting updates on its occupying army, and announcing victories in battles against revolutionaries — throughout the war, Algerians reversed this equation by co-opting wireless bands to share messages of the Revolution and communications between anti-colonialist groups. Highlighting the growing significance of the technology throughout the Revolution, Fanon explained: “Since 1956 the purchase of a radio in Algeria has meant, not the adoption of a modern technique for getting news, but the obtaining of access to the only means of entering into communication with the Revolution, of living with it.”²⁹ This transformation of the radio’s role in the war occurred over the span of fewer than five years, and Fanon recounted that by the late 50s, French forces struggled to block revolutionary broadcasts and to find open channels for their own communications. Fanon’s depiction of how essential the radio became in Algerian life thanks to its role in the Revolution underlines the flexibility of the relationship between particular technologies and public opinion .

This brief example of how radio transformed from an element of the colonial status quo into a key organizing tactic during the Algerian Revolution clearly challenges the notion that the Internet’s potentially democratizing effects are unique to the technology. And as this example demonstrates, even in cases where a particular technology initially appears purely to sustain the existing power structures in a given society, major shifts in the cultural norms surrounding the technology can correspond to equally drastic changes in the scale and nature of its perceived potential impacts. But despite countless instances of particular technologies playing key roles in facilitating the communications necessary for triggering popular uprisings from throughout

history, some aspects of the Internet do set it undeniably apart from previous information and communication technologies (ICTs).

Perhaps the most significant and novel quality of the Internet is the international structure of the many interconnected networks underlying the technology. Cables running across the ocean floor, data passing between satellites, and bits flowing through international Internet Exchange Points (IXPs) do not know or care when they have crossed a national border. In fact, from an Internet governance perspective, individual countries resemble states in a republic more closely than they do distinct nations, in that transnational digital platforms and non-localized data sharing protocols resemble a form of federal authority dictating the policies and norms that shape the global digital space. Continuing with this the metaphor, consider that thirteen US states recently passed their own privacy laws after President Trump revoked Federal Communication Commission's authority to prevent Internet service providers from selling users' information, including location, app and web history. Along similar lines, when players in international Internet governance — such as the Internet Corporation for Assigned Names and Numbers, a non-for profit responsible for managing the domain name system (DNS) — enact new policies or alter protocols, it can impact access to digital platforms across the world, not just in ICANN's country of origin (as was the case after ICANN introduced new top-level domains in 2012).³⁰ Both of these examples demonstrate the multiplex layering of authority and power in different regions and at different levels of Internet governance. We will return to discuss Internet governance hierarchies in greater detail in the next chapter.

In addition to providing states and corporations with immense powers in network hierarchies, the global nature of the Internet may also be of particular interest to technophiles

touting the Ghonim thesis, as countless examples indicate that a system dealing with data and information — technically blind to national borders — can be used to transcend circumvent forms of censorship and repression on the platform. In China for instance, domestic users can bypass the “Great Firewall” government Internet censorship system with a virtual private network (VPN), by masking their I.P. addresses to appear to be connecting from, say, Japan, or any other region outside the jurisdiction of the Chinese filters. VPNs can be expensive and technically difficult to maintain, but mainland Internet users in China have few other options for bypassing government’s tight control over Internet content. VPNs encrypt data on the user’s device before connecting to the ISP, routing all of the user’s traffic through a secure network before decrypting it to process the request, and re-encrypt responses before transmitting them back to the user’s device, where the corresponding VPN software can then decrypt that data in order to display, say, Facebook.com, or any other content that would otherwise be blocked.³¹ Scholars concerned with government regulations over Internet traffic often point to VPNs as a key strategy for combating censorship, with one journalist going as far as to state: “With VPNs, we are all entitled to free speech.”³² As I mentioned however, average users typically lack the knowledge and resources necessary for setting up a VPN, meaning that for most people, their Internet traffic remains subject to regional jurisdiction. Fortunately however VPNs are not the only method for activists to capitalize on the global nature of the Internet.

For many years, including before the Arab Spring, leaders and representatives at companies like Facebook, Google and Twitter have pushed narratives that even the most basic applications of Internet tools can promote human rights and other liberal ideals. In particular, US-based tech companies frequently laud activists’ uses of their services in parts of the world

where the Internet can symbolize a weapon against censorship, underlining the benefits associated with an inherently international platform and fortifying digital platforms' discursive compatibility with the international human rights regime. Consider Youtube in Venezuela, for example. In the midst of a series of violent public protests in May, 2007, President Hugo Chavez announced that Venezuela's Radio Caracas Television (RCTV) network — “the country's oldest and (until recently) most-watched television network,” — would be replaced with a state-run news channel at the end of the month.³³ Covering ensuing protests related to the sanctions threatened against RCTV, a BBC reporter suggested that for critics of the president in Venezuela, “the removal of this voice of dissent is just one more step along a path to dictatorship.”³⁴ Still, the government's decision signified a critical step in this path. Before the change went into effect, *Human Rights Watch* announced, “The Venezuelan government's politically motivated decision not to renew a television broadcasting license is a serious setback for freedom of expression in Venezuela.”³⁵ The outcry over Chavez' announcement that RCTV would be pulled tellingly points to the significance of communications networks and media to revolutionary activities, echoing Fanon and many others, and foreshadowing similar accounts of the Arab Spring three years later. But despite widespread condemnation from local journalists and international human rights organizations — plus “tens of thousands” of protesters marching through the streets³⁶ — on May 27, RCTV's cable license expired, and a state-run news network started broadcasting over the same channel. A major blow to freedom of expression and information in Venezuela, and a testament to the state's power to co-opt traditionally private broadcasting networks. But also, perhaps, an opportunity?

The next day, on May 28 ... well, I should let Google's clever press team to take it from here: "[...] RCTV's news department — operating on reduced staffing — created a channel on YouTube on which it began airing daily three hour-long installments of its newscast 'El Observador.'" By shifting its distribution operations to Google's recently-acquired online video streaming platform, the local opposition news channel had successfully bypassed the state's efforts to block access. (And they did so without any fancy VPN software.) Recognizing a ripe opportunity for cementing the company's public position on government censorship, a month later the "Public Policy Blog" at Google nostalgically recounted the events in Venezuela:

At the risk of sounding like a broken record, one of our policy aims is expanding free flows of information around the world, and advancing the practical ability of users to express themselves. The Internet can clearly be a powerful tool for diverse voices to speak and be heard.

Overly optimistic? Maybe. But consider the example of Venezuela's Radio Caracas Television (RCTV), the country's oldest and (until recently) most-watched television network. One month ago today, we welcomed RCTV and its channel *elobservadorlinea* as a new broadcaster on YouTube.³⁷

Despite not having shown any particular interest in Venezuela censorship before RCTV created its new YouTube channel, Google slickly capitalized on the story to say: "¡Bienvenido a YouTube!", positioning itself as a long-standing advocate and supporter of free speech in the face of government censorship not only on Internet, but across various different communications media and platforms.

Did the author of this Google blog post, like Wael Ghonim, believe that the Internet symbolizes a medium fundamentally freer from government restriction than cable TV? This appears to be the implication, especially in consideration of the technical differences between cable — typically a domestic network system — and the Internet — an international phenomenon. As an Android user and a Google fan myself, I am tempted to entertain the company's postulation here, and in other cases, that its services provide a uniquely unfiltered platform for political dissidents, where older technologies remain more susceptible to state censorship. But examination of the language and timing of Google's statement — not to mention the company's failure to address repeated blocks against the entire YouTube website in the country in recent years, as we will see shortly — reveals a closer resemblance to what business ethicist George G. Brenkert calls a process of “moral compromise” for tech companies around the globe to tow a line between complicity and dissent when operating in countries where the government engages in blatant forms of censorship.³⁸

A decade later, the government in Venezuela appears to have learned its lesson when it comes to effective censorship, and social media companies as a result face much more complex landscapes for attempting to position themselves on the side of free speech. After the state pulled CNN off the air from cable networks in February, 2017, Andrés Eloy Méndez — director of the national telecommunications regulator National Communications Commission (CONATEL) — announced plans to also block the ‘*CNN en Español*’ YouTube channel.³⁹ Although no official block of this nature ever took place, over the following year, the government engaged in repeated acts of temporary, and often apparently arbitrary censorship, blocking specific websites or parts of websites for short periods of time in the country. For example, *Freedom House* reported that

for approximately one hour on June 28, 2017, Internet users in Venezuela were blocked from accessing “several social media platforms — including Facebook, Twitter, YouTube, and Periscope,” and in the same year, the country’s rating dropped from “Partly Free” to “Not Free” on *Freedom House*’s “freedom on the net” global scoring system.⁴⁰ How have US-based digital platform companies responded to these developments?

While Venezuelan journalists and activists, plus international human rights and Internet rights organizations⁴¹ have sharply criticized the recent increase in arbitrary internet blockages in Venezuela, the companies whose services were affected (Facebook, Google and Twitter) issued no statements, and failed to publicly acknowledge the recent spike in state censorship in the country. When, if ever, are companies like Google and Twitter bound to a set of free speech principles? Only when it is convenient? Under what circumstances, and on what legal or moral grounds, can they be held accountable for protecting freedom of speech, or for complying with censorship?

In addition to subtler acts of Internet traffic repression in the country, CONATEL also continues to engage with more blatant and transparent forms censorship, similar to the President’s public announcement concerning the block against RCTV in 2007. Director Méndez regularly appears on state-controlled cable channels to warn other news organizations against covering public protests, and CONATEL has also filed a handful of official takedown requests with US-based social media companies, aimed at specific photos or posts. Unlike the arbitrary or temporary filters outlined in the *Freedom House* report, these more official forms of Internet traffic manipulation present digital platform operators with the chance to reaffirm their commitments to human rights and freedom of speech: published transparency reports from

Google and Twitter expose the takedown requests from different branches of government operating through CONATEL in the last five years.⁴² Out of six government requests for information about specific user accounts filed with Twitter since 2012, the company reports a zero percent compliance rate,⁴³ while Google's transparency reports indicate a similar pattern of noncompliance with takedown requests and requests for user information. As with RCTV's migration onto YouTube, these public stances further highlight the degree to which digital platform companies strive to appear not just reactive, but proactive in dealing with censorship.

In its official transparency report, Google explains how various forms of Internet content takedown requests implicate different concepts and procedures for the company to apply in considering the complaints:

Some requests may not be specific enough for us to know what the government wanted us to remove (for example, no URL is listed in the request), and others involve allegations of defamation through informal letters from government agencies, rather than court orders.⁴⁴

With insights from these transparency reports, we introduce a new form of censorship, whereby digital platforms operators decide internally whether to accept or deny formal requests to manipulate Internet traffic. But these reports show only one part of the story. Twitter's report for instance notably omit reference to cases where the company removed posts or accounts for violating Twitter's Terms of Service (i.e. without any official 3rd-party takedown request). It is perhaps not surprising that companies tend to shy away from including these data in their public reports: private discretionary authority over content moderation signifies increased accountability — or liability — for the companies involved.

Unlike state-sponsored censorship, internal content moderation procedures open social media companies up to accusations of political bias, as we have seen here in the US in recent years. In Venezuela, too, accusations of political bias against digital platform operators provide political leaders with a convenient target for offsetting blame for censorship or traffic manipulation — for example, when Venezuelan president Nicolás Maduro Moros called Twitter “an expression of fascism” last June, as quoted in *Reuters*:

“Twitter in Venezuela today deactivated thousands of people’s accounts,” Maduro said at televised rally. “Simply for being ‘Chavistas,’” he said, using the term for followers of his predecessor, late socialist leader Hugo Chavez.

Chavez was a pioneer among politicians in the use of Twitter, gathering millions of followers and frequently announcing news on the platform. Even today, Chavez’s 4 million followers beat Maduro’s 3 million.

Maduro encouraged a pro-government journalist to publish photos of the head of Twitter in Venezuela, to show people “who was responsible for the manipulation.” It was not immediately clear if Twitter has employees in Venezuela.⁴⁵

Twitter never publicly acknowledged the incident, but journalists speculated that it removed the government-run accounts (actually, only 180 accounts, not “thousands,” were removed) based on violations against the company’s policies.⁴⁶ That the company never explained, or even admitted to, blocking these government officials’ accounts is disturbing insofar as it allows state officials to convert moments like these into populist rallying cries — “Venezuela would respond by opening ‘10,000 or more’ accounts in response, Mr. Maduro insists” — wherein censorship

inversely leads to increased attention or public exposure for a popular movement or politician.⁴⁷ Of course, 10,000 pro-Maduro accounts were probably not what observers had in mind when a journalist in 2014 speculated, “Venezuela's revolution will be Tweeted,”⁴⁸ though platform has indeed proven a pivotal battleground both for freedom of expression in country.

So far I have described or alluded to three technically distinct ways to manipulate Internet traffic flow. The first, characterized by direct overt censorship by the state, presents nondomestic digital platform companies like Google and Twitter with crucial opportunities to publicly reaffirm their commitments to freedom of expression. These circumstances arise both when the government’s managerial authority over older technologies exceeds its control over the Internet (as in the case of RCTV, and in support of the Ghonim thesis), and when governments go through platform operators’ official channels to file takedown requests (as indicated in the companies’ transparency reports). This form of manipulation will prove especially significant throughout the next two chapters, where I argue that the conceptual relationships between human rights scholarship and private actors in ICT industries often rely heavily on traditional notions of freedom of expression.

A second form of manipulation over public access to information on the Internet illustrated thus far comes in the form of more arbitrary or discrete acts of censorship, wherein governments or corporations may temporarily block access to certain websites, pages or accounts without publicly acknowledging the act. Although cases like these often remain formally unacknowledged, as with more traditional forms of repression described in the previous paragraph, the consequences are undeniable — for example, when the government in Venezuela

managed to temporarily block images from appearing on Twitter's website following bloody anti-government protests in 2014⁴⁹ — providing potent ammunition for targets of the attacks to claim victimhood of repression or political bias. China's "Great Firewall" could be categorized in either of these first two forms of manipulation, depending on which components of the system we focus on. Consider that it is not illegal in China to access blocked websites, it is simply very difficult; meaning Internet optimists can still point to VPNs or other alternative methods for connecting as evidence in support of the Ghonim thesis (i.e. there is no VPN equivalent for cable TV networks).⁵⁰ Taken in another light however, the Great Firewall more closely embodies a form of covert censorship, given that the government in China provides no official or public description of what is and isn't allowed on the Internet.

Both aforementioned forms of Internet traffic manipulation intersect directly with another theme, previously discussed, on the inherently global nature of the technology. In all of the examples described in the previous two paragraphs, censorship can be bypassed thanks to the international links between networks that transcend national boundaries and traditional state jurisdictions. Highly nationalized Internet governance infrastructures like that in China — or in Venezuela, for example, where *Freedom House* estimated out that "the government may control roughly 60 percent of the national-level backbone infrastructure" for Internet services — mean governments possess much more direct control over transnational traffic there than in the United States, for example. In this sense, as we will later see, Internet governance structures in countries like the US provide crucial beacons of hope to idealists dreaming of an unfettered Internet, while also providing a critical a counterbalance and alternative point of connection for users in regions where blatant Internet censorship is the norm.

Now you may be wondering: How did the Internet in the US develop into such a beautifully free and open platform, home to an industry of social media companies credited with enabling the Arab Spring, where young citizens coalesced around the nation's first black President, and where dissidents in repressive countries find alternative outlets for expressing criticism? This question leads into our third and final form of Internet traffic manipulation, manifesting in nearly invisible attacks on democracies through mass disinformation campaigns on social media. This third form of censorship is more difficult to define. So rather than attempting to define it, the next two chapters are devoted to illustrating the process by which a comfortable compatibility developed between social media companies and human rights discourse, allowing for this relatively new form of censorship to emerge mostly undetected. As a result, confusion and contention characterize the modern landscape of efforts to apply traditional free speech doctrine to social media companies, while neoliberal pretexts enable digital platform operators to enjoy immense flexibility in how and when they apply language of free speech and human rights. Take, for the final example in this chapter, Apple CEO Tim Cook's explanation of the company's recent decision to remove "all major VPN apps" from the App Store in China:

We would obviously rather not remove the apps, but like we do in other countries, we follow the law wherever we do business. We strongly believe in participating in markets and bringing benefits to customers is the best interest of the folks there and in other countries as well.^{51, 52}

The will to resist government censorship is purported, if only weakly in some cases, but consistently and usually in reference to some concern for the greater good among prominent actors and leaders in the tech industry. Here for instance, Cook suggests that although removing

VPN apps goes against free speech ideals, the decision ultimately proved necessary for the company to continue operating in China. But how does Cook's emphasis on importance of "participating in markets" weigh against internal decisions at digital platforms companies to comply or oppose government censorship? And more importantly, at what point did US-based companies acquire the legal and moral leeway to "follow the law" in countries where the law is blatant censorship?

Chapter 1 Notes

1. Statista. "U.S. Population With A Social Media Profile 2018." 2018.
<https://www.statista.com/statistics/273476/percentage-of-us-population-with-a-social-network-profile/> (accessed December 7, 2018).
2. Carr, David. "How Obama Tapped Into Social Networks' Power." *The New York Times*, November 8, 2008. <https://www.nytimes.com/2008/11/10/business/media/10carr.html> (accessed December 10 2018).
3. Frasier, Matthew and Soumitra Dutta. "Obama's Win Means Future Elections Must Be Fought Online." *The Guardian*, November 7, 2008.
<https://www.theguardian.com/technology/2008/nov/07/barackobama-uselections2008> (accessed December 10 2018).
4. Smith, Aaron. "The Internet's Role In Campaign 2008." Pew Research Center (2009).
<http://www.pewinternet.org/2009/04/15/the-internets-role-in-campaign-2008/> (accessed December 10, 2018).
5. Miller, Claire. "How Obama's Internet Campaign Changed Politics." *The New York Times Bits Blog*, November 7, 2008.
<https://bits.blogs.nytimes.com/2008/11/07/how-obamas-internet-campaign-changed-politics/> (accessed December 10 2018).
6. Slotnick, Allison. "'Friend' the President: Facebook and the 2008 Presidential Election." In *Politicking Online: The Transformation of Election Campaign Communications*, edited by Panagopoulos Costas, 249-71. New Brunswick, NJ; London: Rutgers University Press, 2009. <http://www.jstor.org/stable/j.ctt5hj455.18>.
7. Ibid., 269.
8. Castells, Manuel. *The Information Age: Economy, Society, and Culture*. Chichester, West Sussex: Wiley-Blackwell, 2010. <https://books.google.com/books?id=hngg4aFtJVcC>
9. Floridi, Luciano (2012). *The Fourth Revolution*. *The Philosophers' Magazine* 57: 96-101.
<https://philpapers.org/rec/FLOTFR>
10. Chun, Wendy Hui Kyong. Eds. Anna Watkins Fisher and Thomas Keenan. *New Media, Old Media: A History and Theory Reader*. New York: Routledge, 2016.
11. Ibid., 40.
12. 269 Slotnick, "'Friend' the President: Facebook and the 2008 Presidential Election."
13. Thomas J. Johnson & David D. Perlmutter (2010) Introduction: The Facebook Election, *Mass Communication and Society*, 13:5, 554-559, DOI: 10.1080/15205436.2010.517490 (PDF) *Introduction: The Facebook Election*. Available from:
https://www.researchgate.net/publication/254306502_Introduction_The_Facebook_Election (accessed December 10, 2018).
14. Slotnick, "'Friend' the President: Facebook and the 2008 Presidential Election."

15. Interviewee Schrage, Elliot. "New Media Tools and Public Diplomacy." Interview by Lee Hudson Teslik. *Council on Foreign Relations*, May 4, 2009
<https://www.cfr.org/interview/new-media-tools-and-public-diplomacy> (accessed December 10, 2018).
16. LoGiurato, Brett. "Mitt Romney Has A New Strategy To Dominate The Facebook Campaign Wars." *Business Insider*, June 18, 2012.
<https://www.businessinsider.com/mitt-romney-campaign-facebook-social-media-zac-moffatt-barack-obama-2012-6> (accessed December 10, 2018).
17. Facebook Politics & Government Team. "Facebook Apps Bring the Power of Friends to the Political Process." Facebook Post, August 30, 2012, 12:52 pm.
<https://www.facebook.com/notes/government-and-politics-on-facebook/facebook-apps-bringing-the-power-of-friends-to-the-political-process/10150994792695882/> (accessed December 10, 2018).
18. Cillizza, Chris "What the 2012 Election Taught Us." *The Washington Post*, November 7, 2012.
https://www.washingtonpost.com/news/the-fix/wp/2012/11/07/what-the-2012-election-taught-us/?utm_term=.151f90df7b3b (accessed December 10, 2018)
19. Pilkington, Ed, and Amanda Michel. "Obama, Facebook And The Power Of Friendship: The 2012 Data Election." *The Guardian*, February 17, 2012.
<https://www.theguardian.com/world/2012/feb/17/obama-digital-data-machine-facebook-election> (accessed December 10 2018).
20. Ibid.
21. Ibid.; Hellweg, Eric. "The First Big Data Election." *Harvard Business Review*, November 13, 2012
22. Scherer, "Friended: How The Obama Campaign Connected With Young Voters"
23. Williams, Christin B. and Girish J. Gulati. "The Political Impact of Facebook: Evidence from the 2006 Elections and the 2008 Nomination Contest." In *Politicking Online: The Transformation of Election Campaign Communications*, ed. Panagopoulos Costas, 272-91. New Brunswick, NJ; London: Rutgers University Press, 2009.
<http://www.jstor.org/stable/j.ctt5hj455.19.>; Talbot, David. 2012. "Facebook: The Real Presidential Swing State." *MIT Technology Review*, July 20, 2012.
<https://www.technologyreview.com/s/428530/facebook-the-real-presidential-swing-state/> (accessed December 10, 2018).
24. Hellweg, "The First Big Data Election."
25. Guardian Online. "Team Obama eyes FB as trump card." *The Daily Star*, February 19, 2012.
<https://www.thedailystar.net/news-detail-223039> (accessed December 10, 2018).
26. Rao, Leena. "Detained Egyptian Google Marketing Exec Wael Ghonim Released." *Techcrunch*, February 7, 2011.

27. Ghonim, Wael. Quoted in Doran, Michael S. et al. "The Impact of New Media: The Revolution Will Be Tweeted." In *The Arab Awakening: America and the Transformation of the Middle East*, 39-46. Brookings Institution Press, 2011.
<http://www.jstor.org/stable/10.7864/j.ctt1280ww.9> (accessed December 7, 2018).
28. Armbrust, Walter. "The Revolution Against Neoliberalism." In *The Dawn of the Arab Uprisings: End of an Old Order?*. ed. Haddad Bassam, Bsheer Rosie, and Abu-Rish Ziad, by Owen Roger. London: Pluto Press, 2012: 122. doi:10.2307/j.ctt183p77h.23.
29. Fanon, Frantz. *A Dying Colonialism*. New York: Grove, 1967: 75.
30. Arthur, Charles. "Icann Announces Huge Expansion Of Web Domain Names From 2012." *The Guardian*, June 20, 2012. Accessed December 10 2018.
<https://www.theguardian.com/technology/2011/jun/20/icann-domains-expansion-announced> (accessed December 10, 2018).
31. Friesland, Kees. "How to Use VPNs in China Without Breaking the Law – Understanding The Technicalities." TachNadu, September 6, 2018.
<https://www.technadu.com/how-to-use-vpns-in-china-without-breaking-the-law/18492/> (accessed December 10, 2018).
32. Gidali, Sagi. "If we want free speech across the globe, we need VPNs." The Daily Dot, Mar 17, 2016.
33. Jaitly, Rishi. "Welcome to YouTube, RCTV!" Google Public Policy Blog, Thursday, June 28, 2007. <https://publicpolicy.googleblog.com/2007/06/bienvenido-youtube-rctv.html> (accessed December 10, 2018).
34. Ingham, James. "Venezuelans Protest Over TV Issue." BBC News, Caracas, May 27 2007. <http://news.bbc.co.uk/2/hi/americas/6695769.stm> (accessed December 10, 2018).
35. Human Rights Watch. "Venezuela: TV Shutdown Harms Free Expression." May 21, 2007. <https://www.hrw.org/news/2007/05/21/venezuela-tv-shutdown-harms-free-expression> (accessed December 10, 2018).
36. Ellsworth, Brian. "Venezuelans March Against Closure of TV Station." Reuters, May 26, 2007.
<https://www.reuters.com/article/us-venezuela-television-march/venezuelans-march-against-closure-of-tv-station-idUSN2621739620070526> (accessed December 10, 2018).
37. Jaitly, "Welcome to YouTube, RCTV!"
38. Brenkert, George G. "Google, Human Rights, and Moral Compromise." *Journal of Business Ethics* 85, no. 4 (2009): 453-78. <http://www.jstor.org/stable/40294808>.
39. Freedomhouse.org. "Venezuela Country Profile." Freedom on the Net 2017.
<https://freedomhouse.org/report/freedom-net/2017/venezuela> (accessed December 10, 2018).
40. Ibid.

41. Human Rights Watch. "Venezuela: Events of 2017." 2018. <https://www.hrw.org/world-report/2018/country-chapters/venezuela#> (accessed December 10, 2018).
42. Google. "Traffic and Disruptions to Google." Transparency Report. https://transparencyreport.google.com/traffic/overview?disruption_history=product:21;size:4&lu=disruption_history (accessed December 10, 2018).
43. Twitter. "Removal Request." Transparency Report. <https://transparency.twitter.com/en/removal-requests.html> (accessed December 10, 2018).
44. Twitter. "Government Requests to Remove Content." Transparency Report. https://transparencyreport.google.com/government-removals/by-country/VE?country_request_amount=group_by:branches;authority:VE&lu=country_request_amount (accessed December 10, 2018).
45. Daniel, Frank Jack. "Venezuela's Maduro Slams Twitter After Accounts Blocked." Reuters, June 17, 2017. <https://www.reuters.com/article/us-venezuela-politics-twitter/venezuelas-maduro-slams-twitter-after-accounts-blocked-idUSKBN1980U1> (accessed December 10, 2018).
46. Fingas, Jon. "Twitter Blocks a Slew of Venezuela Government Accounts." Engadget, June 19, 2017. <https://www.engadget.com/2017/06/19/twitter-blocks-venezuela-government-accounts/> (accessed December 10, 2018).
47. "Twitter blocks 180 Accounts of Venezuela Government; Maduro Stays Defiant." *The Santiago Times*, June 19, 2017. <https://santiagotimes.cl/2017/06/19/twitter-blocks-180-accounts-of-venezuela-government-maduro-stays-defiant/> (accessed December 10, 2018).
48. Friedman, Uri. "Why Venezuela's Revolution Will Be Tweeted." *The Atlantic*, February 19, 2014. <https://www.theatlantic.com/international/archive/2014/02/why-venezuelas-revolution-will-be-tweeted/283904/> (accessed December 10, 2018).
49. AP. "Twitter Reports Image Blocking in Venezuela." *USA Today*, February 14, 2014. <https://www.usatoday.com/story/news/world/2014/02/14/twitter-image-blocking-venezuela/5497219/> (accessed December 10, 2018).
50. Stephens, Zoe. "What is a VPN, and is VPN illegal in China?" LTL Mandarin School Blog, May 14, 2018. <https://ltl-school.com/vpn-illegal-china/> (accessed December 10, 2018).
51. Hill, Rebecca. "Apple Chief on Chinese VPN App Ban: We Always Toe the Line with Other Nations' Laws." *The Register*, August 7, 2017. https://www.theregister.co.uk/2017/08/02/apple_chief_on_chinese_vpn_app_ban/ (accessed December 10, 2018).
52. Clark, Bryan. "No, Apple isn't 'enabling' Chinese censorship." *TheNextWeb*, October 20, 2017.

Chapter 2: Moralizing Internet Governance Theory

(Or, Watch the Internet Derail Human Rights)

This chapter appends technical excerpts to a literature review submitted to professor Peter Rosenblum for the Human Rights Junior Seminar course in Spring 2017. Text from the original literature review appears in the Times typeface, while new excerpts appear in Arial. Original text should not be considered part of my Senior Project. The appended excerpts fill gaps where I was restricted in the literature review from drifting too far off from mainstream rights scholarship. The purpose of this chapter is to demonstrate how the privatization of Internet governance theory in the 1990s and early 2000s corresponded to the mainstream human rights regime fundamentally narrowing in scope, whereby private sector power in Internet governance grew to dominate not just physical but also conceptual and moral landscapes.

Introduction

For decades, human rights theorists have explicitly identified a conceptual relationship between globalization, human rights and information & communications technologies (ICTs). Scholars today grappling with the impact of the Internet on human rights work still often turn back to the UN Secretary General's 1992 "Agenda for Peace," in which Boutros Boutros-Ghali forecasted potentially drastic changes:

Technological advances are altering the nature and the expectation of life all over the globe. The revolution in communications has united the world in awareness, in aspiration and in greater solidarity against injustice. But progress also brings

new risks for stability: ecological damage, disruption of family and community life, greater intrusion into the lives and rights of individuals.¹

Despite giving this speech before the modern Internet existed, the Secretary General acutely warned that new technologies communications technologies could be dual-edged in their impact on the human rights project. Ghali's relatively inexplicit account of networking technologies however reflected a broader trend among rights scholars in the early 90s to shy away from more technical attempts at understanding and responding to this "revolution in communications."

Few within the mainstream human rights community tackled the Internet from a conceptual standpoint until later in the 90s, although for decades, projects like Human Rights Internet employed related technologies to share information digitally across national borders. Founded in 1976 in Ottawa, Canada, Human Rights Internet compiles data from rights advocacy groups, allowing users to track and share the work of NGOs across the globe.² In contrast to later projects (and before most people used the Internet) originally only a handful of academics and journalists could access HRI.³ This project symbolized one of the earliest 'tool-based' human rights schemas for networking technology in that HRI employed networking technology to advance preexisting rights-related goals (in other words, it used particular Internet technologies to support traditional human rights work) rather than addressing risks to human rights principles posed by advances in ICTs more broadly.

NSFNet, CIX

In the same year as Ghali's speech, the U.S. Congress House Committee on Science, Space, and Technology (HCSST) established new conditions for the National Science Foundation's funding of NSFNet, an experimental networking project founded in 1987 to link

supercomputers at five universities across the country. After a day-long hearing, the HCSST determined that NSF would remain involved in the program "primarily for research and education in the sciences and engineering,"⁴ allowing private Internet Service Providers (ISPs) to take over most of the future construction for the infrastructural 'backbone' of a series of connecting networks we now call the internet.⁵ The NSF developed an 'Acceptable Use Policy' in accordance, covering the physical pieces of the network it still owned and operated, which prohibited the use of the 'NSFNet backbone' for "for-profit activities" or the "extensive use for private or personal business."⁶

A handful of commercial organizations had been developing connections between their private networks since 1991, sending NSFNet traffic through the Commercial Internet eXchange (CIX). Inaugurated in Richmond, VA, the CIX established something akin to a free-trade agreement between networks, allowing commercial traffic to flow freely between users with different ISPs. But when the HCSST forbade commercial use of NSFNet in 1992, the federally-funded infrastructure of the NSF — still intertwined with emerging private networks — rendered commercial traffic passing through the NSFnet unreliable and legally questionable.⁷ Furthermore the CIX started enforcing a \$10,000 fee for regional networks to gain access to what was at the time the only major interexchange point open for commercial use.⁸ These setbacks to the private sector's ability to exploit the technology proved significant, but impermanent, and symbolized an early stepping stone in the privatization of the Internet.

The Right to Communicate

Other branches of human rights work preceding the advent of the Internet benefited from a more heterogeneous coalition of supporters, and pursued more wide-ranging and ambitious goals related to communications technologies. For example, the UN Economic Commission for

Africa (ECA) co-founded The Pan African Development Information System (PADIS), a program to support the development of ICT infrastructures in the region.⁹ The ECA called for the Secretary General to approve PADIS in a letter on March 22, 1980, describing access to ICTs as an enabler for other rights:

[A] self-sustaining and self-reliant pan-African development policy which has among its primary objectives self-sufficiency in food, the development of its natural and human resources, the promotion of intra-African trade and the intensification of industrial development can be conducted properly only if it is supported by a sound documentation and information system.¹⁰

Whereas HRI focused specifically on accessibility to human rights documentation, PADIS would have applied to making the Internet itself more accessible. In this sense PADIS complemented the broader “New World Information and Communication Order” (NWICO) movement, a platform UNESCO popularized in the early 1980s, based around “The Right to Communicate.”¹¹ Efforts related to the “Right to Communicate” largely framed access to ICTs in terms of physical infrastructure, while addressing issues of content and censorship with concern to the monopolistic corporate power of media operations in the developed world.¹² Both PADIS and HRI worked to increase access to at least some form of information network internationally.

Stemming from discussions in 1976 at the 19th General Conference of UNESCO in Nairobi, Kenya, NWICO gained widespread support among developing nations in the “global south” over the following decade.¹³ In accordance with the first “cornerstone” of the platform — democratization — NWICO highlighted the importance of journalistic freedom and the “free flow of information” globally for achieving this goal.¹⁴ As a part of this pursuit, NWICO

included “the obligation of the international organizations to assist the non-aligned countries towards the emancipation and development of their national information systems.”¹⁵ UNESCO almost single-handedly brought the concept into the mainstream in the early 80s by advocating for the “New World Information and Communication Order” platform (NWICO), wherein the Right to Communicate played a central role.¹⁶

Scholars pointed out that Western nations mostly resisted the Right to Communicate for fear that it and NWICO “implied a kind of international obligation to provide a means for people to communicate that states in either the First or Third Worlds had neither the resources nor will to support or subsidize.” To promote pluralism in media, NWICO also entailed “a reduction of the monopoly power of existing transnational media,” likely aggregating resistance to the practical implications of the platform.¹⁷ Highlighting additional symptoms of the inefficient program, African scholars throughout the 1980s called for greater funding and support through PADIS and complained of a bureaucratic process burdened by fragmentation and circularity.¹⁸

The Right to Communicate relied on direct government involvement and oversight to expand ICT systems in African nations — with funding from the UN — using the power of states to defend human rights at the cutting edge of the intersection between globalization and networking technologies. In 1982, the Republic of Bénin created the “Centre National Automatisé de Documentation et d’information” (CENADI), a government program to establish “a national information network in order to sustain the country’s economic and social development,” with funding from the UN through PADIS.¹⁹ Initially, the “public had free access to the holdings of the CENADI and its databases,” and the center offered computer and software training to citizens of Bénin. Gradually however, aspects of the CENADI database were “legally

suppressed,” and the project became more of a “documentation center” solely for the Ministry of Planning, Statistics, and Economic Analysis, the Béninese government body behind CENADI.²⁰ In 1989, academics in Bénin reported that the CENADI had completely failed and disappeared due to “administrative instability” in its implementation with the state.²¹

Bénin was not the only failed attempt to implement ICT construction programs through the ECA and the UN. Demonstrating the shortcomings of projects related to the Right to Communicate empirically, a 1995 case study on PADIS in Zambia showed the UN program to be ineffective.²² Not only did few people know of its existence in the country, but “hardly any publications were being produced for the PADIS project.” More generally, the study argued, “African countries were not ready to undertake the PADIS project because they lacked clear strategies for its implementation.”²³ This early account foreshadowed patterns of contention between human rights scholars about how to implement Internet technologies concerning disagreements over whether obstacles could be attributed to “technical problems” or “policy issues.”²⁴

Scholars offered varying explanations for why the program failed in different countries, but most agreed that NWICO and the Right to Communicate ultimately met their ends after the US and Britain withdrew from UNESCO in 1984 and 1985 respectively. The countries “mentioned UNESCO’s work with NWICO among the reasons for their decision to leave the organization,”²⁵ and less publicly, but more specifically, the United States opposed the project because “the new, proposed order might impose on the operations and practices of global businesses and military intelligence, currently governed almost exclusively by market factors or the raw power of the U.S. military machine.”²⁶ Although it never developed into a cohesive,

standardized set of standards, the global prevalence of the Right to Communicate in the decades leading up to the privatization of the Internet represented a strategy reliant on government cooperation and involvement in the development and implementation of new ICTs.²⁷ Its abandonment by major players in the rights regime and the failure of related projects coincided with growing doubt over the efficacy of a state-led pursuit to ensure that the Internet reflects human rights principles.²⁸

Cyber-Libertarianism, Anti-Communism

Scholars outside the human rights discipline began compiling data on global disparities in Internet access (later dubbed the “North-South Information Divide”²⁹) as early as 1993, providing an indirect response to the UN Secretary General’s call to heed the risks of “disruption” and “damage” new technologies introduced.³⁰ A small group of individuals — fondly remembered as “information-age luminaries” — had extensively explored the ethics, laws and theories concerning networking technologies since the late 1980s.³¹ This community of academics, journalists and technical experts included John Gilmore, Mitch Kapor and John Perry Barlow, co-founders of the Electronic Frontier Foundation (EFF)³²; Esther Dyson, who joined the EFF and later served as the first Board Chair of the Internet Corporation for Assigned Names and Numbers (ICANN)³³; Steven Levy, author of *Hackers: Heroes of the Computer Revolution*³⁴; and among others, *Code as Law* author Lawrence Lessig, a long-time supporter of individual liberty and privacy online.³⁵ In the late 80s and early 90s these scholars spearheaded the “Cyber-Libertarianism” movement, which would gain traction throughout the decade and

become a dominant moral narrative for addressing Internet governance among human rights leaders, members of the private sector and policymakers alike.³⁶

‘Cyber-Libertarian’ scholars employed similar language to that of their human rights counterparts in discussing the potentially adverse consequences of new technology. For instance, an article in the *Communications of the Association for Computing Machinery* (1994) pointed out that “[a]lthough IT in general, and networking in particular, have often been praised as democratizing technologies,” the internet was also already proliferating in countries with “strong internal security regimes and heavy constraints on Western-style civil rights.” Similarly to Boutros-Ghali’s broad warnings in 1992, these cases demonstrated that the Internet is inherently neither democratizing nor harmful to democracy.

Layered on top of this more neutral depiction of the Internet’s potential impact on human rights (common to mainstream discourse at the time), the authors also offered a solution to the problem as they identified it — hoping that Internet growth would be “accelerated by the privatization of telecommunications services,” thereby preventing repressive states from directly controlling the availability of digital information by keeping management in the private sector.³⁷ With this increasingly popular strategy, ‘cyber-activists’ could theoretically support increasing internet access globally by maximizing private power in the industry while minimizing government oversight in the name of free expression and individual privacy.

The Right to Communicate and Cyber-Libertarianism in this sense embodied two opposing visions for the ideal extent of government involvement and regulation over emerging global networks³⁸: The UN asked national governments to assume responsibility for ensuring distributed implementation of new communications technologies,³⁹ while Cyber-Libertarianism

stressed the risks of allowing states to operate and control the Internet. Mainstream scholarship at this time as a result lacked consensus over how to assign responsibility in ICT-related efforts to globalize human rights,⁴⁰ but the collapse of NWICO complemented the rising popularity of a movement to minimize state involvement in networking technology, offering a promising path for leaders in need of a new discourse.⁴¹

Even as older conceptual models in powerful Western nations from before the fall of the Soviet Union — dependent on an East-West, liberal-illiberal, or anti communist–communist paradigm — became less relevant, many scholars remained attached to the idea that repressive governments pose the greatest threat to human rights principles in the international context.⁴² During the Cold War, the US for example — a powerful member of the UN and a leader in foreign aid — oriented its foreign policy primarily around “the goal to contain Communism,” focusing specifically on non-democratic governments.⁴³ As this line faded in the early 1990s, governments in the West increasingly turned to the language of human rights for identifying particular regions as targets for aid, sanctions, or other foreign policy actions. One study found that after the Cold War, US arms transfers started to reflect a negative correlation to nations with documented human rights abuses, compared to a statistically insignificant relationship during the Cold War.⁴⁴ Jack Donnelly eloquently described the role into which human rights stepped, writing: “Foreign policy involves how a state sees itself, the world around it, and its place in that world. The global human rights regime has created a world in which government’s commitment to human rights is seen as essential to full national and international legitimacy.”⁴⁵ Leading up to these more recent developments, the tendency among human rights scholars in the early 90s to focus on governments as the primary threat to digital liberties resembled post–World World II

foreign policy strategies in the West focusing on Communist states. In both models, national governments present the greatest risk to international human rights, making human rights an attractive discourse for states to acquire following the end of the Cold War.

Global disparities in the quality of Internet implementation and access, and private tech companies' ethical and legal obligations in the ICT revolution, remained relatively fringe topics until later in the decade and in the early 2000s, compared to mainstream human rights discussions focusing on traditional versions of state censorship and more ambiguous references to the consequences of networking technology.⁴⁶ Leaders in the field swayed under pressure from a triage of complex factors (the collapse of the Right to Communicate, Cyber-Libertarianism and the end of the Cold War⁴⁷), and as Congress initiated the process of privatizing the Internet in the early 1990s,⁴⁸ the most common accounts of the relationship between globalization and ICTs among mainstream human rights scholars highlighted mystery, caution and possibility.⁴⁹

Commercial NAPs, NSI

To aid in the expansion of commercial networks, in 1994 the NSF awarded grants for Ameritech, Pacific Bell (both of which AT&T later acquired), Sprint and Verizon to construct four Network Access Points (NAPs), in Chicago, San Jose, New York and Washington DC, respectively.⁵⁰ A year later, the National Science Foundation abandoned NSFNet, lifting the remaining restrictions on commercial traffic in the process. The program's nostalgic Final Report stated, "NSFNET backbone service will be remembered not only for achieving the goal of providing networking connectivity to the research and education community but also for realizing some of the larger hopes of the partners:"

that networking would become a ubiquitous part of everyday life for more and more people, and that it would create new markets for products and services in networking and communications, thus promoting technology transfer.⁵¹

With the only reference to “rights” in the report being in the context of privatizing wireless spectrum, the NSF and the HCSST offered relatively idyllic visions for a future in which internet technologies “would become a ubiquitous part of everyday life.” Although the consequences of promoting “technology transfer” as the ultimate value of the program remained unclear, the government’s language proved highly compatible with that of activists who sought to minimize state regulation over the internet.

The CDT

Mainstream rights scholars began working more closely with members of the private sector, technical experts and groups associated with Cyber-Libertarianism in the mid-1990s in campaigns against state attempts to filter Internet content. The Center for Democracy and Technology (CDT) represented one such endeavor; the organization focuses specifically on the Internet to promote “global online civil liberties and human rights,” according to its website.⁵² Jerry Berman founded the CDT in 1994, a few months after leaving the Electronic Frontier Foundation (EFF) — one of the first civil society groups to link networking technology with human rights language in 1990.⁵³ By the mid-90s, the EFF and the CDT stood out as beacons of a more pointed and technical form of inquiry, in contrast to otherwise general uncertainty enveloping many human rights activists concerning ICTs and the Internet.⁵⁴

Berman reportedly left the EFF after “bitter internal disputes” with core members of the organization, who “felt that Berman was working too closely with the government.”⁵⁵ This

schism in Cyber-Libertarian policy advocacy work corresponded to the beginning of direct intersections between the young discourse with mainstream human rights theory. While older organizations like the EFF, led by ‘information-age luminaries,’ primarily focused on “civil liberties” (working to implement US Constitution and Bill of Rights principles into Internet governance), the CDT came to represent a more globalized version of the effort to protect rights online, working in tandem with the UN, member states, and other international human rights organizations. These efforts provided human rights advocates with a crucial ‘in’ to more technical discussions about the Internet than were common in mainstream scholarship before.

In 1996 the CDT and the Open Society Institute organized the first meeting of the Internet Freedom Network (IFN), an international coalition of civil liberties and human rights organizations “to oppose efforts to regulate privacy and free speech on the Internet.”⁵⁶ The IFN meeting, in Toronto, Canada, brought representatives from the United Nations, Human Rights Watch, and states in Africa, Asia, Europe, North and South America together with “public policy specialists from Internet services providers and software companies,” to strengthen agreements on existing ethical and legal frameworks for Internet governance.⁵⁷ Through the IFN, Berman and the CDT catalyzed an unprecedented structure for of cooperation between a) states and corporations involved with Internet governance and b) mainstream rights organizations, human rights scholars and civil liberties advocates.

As rights scholars rubbed shoulders with Cyber-Libertarians in the mid-90s, both discourses also started to acknowledged the increasing power of private corporations in Internet governance.⁵⁸ Covering a broad range of topics related to free speech, surveillance, information accessibility and distributed accountability, the IFN meeting centered around issues concerning

efforts by national governments to regulate an international platform. The group ostensibly resembled PADIS or NWICO, in that the project appealed to global and supranational interests and its work employed examples of disparities in Internet access in different regions of the world. But the INF's list of members suggests it more closely emulated a distinct trend emerging among rights scholars in the mid-1990s endorsing a Cyber-Libertarian philosophy of Internet governance by seeking to minimize the potential for state censorship by shifting ownership of new ICTs into the private sector.⁵⁹

The official summary of the meeting examined a series of technical examples of states censoring Internet content, highlighting the complex legal and ethical relationship between Internet Service Providers (ISPs) and the content to which they provide access. Although ISPs are technically “mere conduits of information or hosts for websites” — and do not generate or own online content — they remain “particularly vulnerable to government intimidation and legally-sanctioned censorship,” the document pointed out.⁶⁰ The summary provided this example of ISP vulnerability: after the government of Zambia banned an edition of the *Weekly Post*, where the opposition newspaper had published a leaked government document, “possession of any copies of the banned material” became a crime in the country.⁶¹ This included digital copies; the government also ordered a local ISP to block the edition on the *Weekly Post* website. Because the newspaper hosted their site on the same ISP, blocking the articles meant preventing access not just domestically, but globally.⁶² The INF's inclusion of this example marks one of the earliest examples of an international organization representing human rights acknowledging the weight private distribution networks carry in instances of government Internet censorship.

The case in Zambia ended relatively fortunately, simultaneously demonstrating a potential weapon against censorship borne in networking technology: “before the banned articles were removed from the Zambian Web site, an Internet user in the United States downloaded the material. The banned articles are still available on web servers in other African countries and the United States.”⁶³ A group of human rights journalists writing in the early 2000s dubbed the mirroring of the *Weekly Post* articles a “victory for media pluralism, aided by communications technology.”⁶⁴ Highlighting optimistic narratives like this one — on the balance between censorship and free speech online — remains a popular strategy among entrepreneurial members of the tech industry and human rights field alike.⁶⁵ Still, the meeting summary painted a clear picture at the time: many examples demonstrated that the Internet offered governments a powerful new tool for censorship and surveillance. Perhaps more importantly, these scholars also identified the complicated relationship between private ISPs and state attempts to censor Internet traffic.

Mounting evidence of states and private organizations suppressing Internet content rang alarm bells for free speech advocates, and by the mid-90s a growing body of scholars raised questions about how to protect the First Amendment on the Internet in the US and globally.⁶⁶ The Center for Democracy and Technology in the eyes of mainstream human rights scholars represented a vital pioneer in technical approaches to linking networking technologies with human rights, particularly free speech.⁶⁷ Although similar efforts to cohere models for Internet governance with anti-censorship principles had been underway for a decade or more in Cyber-Libertarian circles, the CDT represented one of the earliest attempts to bring technical

conversations about the Internet and human rights into the context of international political relations and commerce, including members of the private, public and non-profit sectors.

Cooperative Models

The process of transposing human rights language onto the private sector to accommodate for the growing power of corporations in the emerging digital realm gained even more traction in the late 1990s through a series of legal battles in the United States over attempts by the government to regulate the Internet. In its pursuit against censorship, the CDT fought against the Communications Decency Act (CDA) of 1996 — a bill expanding legislation covering radio and television to include the Internet — which granted the Federal Communications Commission (FCC) extensive regulatory control over the new technology,⁶⁸ prohibiting “obscene” or pornographic material online.⁶⁹ The American Civil Liberties Union, the CDT, the EFF, and other groups opposed the legislation, contending that the measure violated free speech principles. Some also complained that the legislation would have adverse consequences for Internet users outside the US: “The CDA would permit the U.S., for example, to seek the arrest of a European content provider whose sexually explicit material was seen as ‘indecent’ or ‘patently offensive,’” warned Human Rights Watch.⁷⁰

In June 1997, in the wake of mounting criticism from civil liberties groups, the private sector, and human rights scholars and organizations, the Supreme Court struck down the sections of the CDA prohibiting “indecent” content. *Reno v. ACLU* constituted the culmination of a series of legal battles led by the ACLU and the Citizens Internet Empowerment Coalition — a group the CDT created to combat the CDA, including more than 30,000 members in “the mainstream

American publishing and content distribution community, and the Internet community itself⁷¹ — in the months leading up to the Supreme Court’s decision, resulting in a major blow to the FCC’s regulatory power over the Internet. Human Rights Watch, a handful of ISPs and tech companies including America Online (AOL), Apple and Microsoft, plus civil society groups like Computer Professionals for Social Responsibility, the Journalism Education Association and Planned Parenthood of America,⁷² all served as plaintiffs in *Reno vs. ACLU*, demonstrating one of the earliest instances of mainstream human rights and civil society groups working directly with commercial interests (the CDT co-directed the CIEC with AOL) to combat government Internet regulation.

Thus far, I have depicted three phases in the history of applying human rights concepts to early networking technologies. The first, characterized by NWICO and the Right to Communicate, sought to promote global equality in access to ICTs by involving states from both the developing and the developed world with projects to support infrastructure construction and oversight of information technologies. Cyber-Libertarianism, in contrast, focused on states as the greatest threat to human rights online, often opposing any and all government involvement with the implementation or maintenance of networking technologies. Although not originally linked to mainstream human rights scholarship, even the earliest Cyber-Libertarians shared principles, strategies and vocabulary with human rights traditions, particularly on notions concerning free speech and government censorship.

A continuation of both the Right to Communicate and Cyber-Libertarianism, the Center for Democracy and Technology exemplifies the third phase in this history: a hybrid model for Internet governance dealing with the threat of state regulation by advocating for little to no

government oversight while emphasizing privatization. Unlike previous work by members of the Cyber-Libertarian tradition, the CDT explicitly employed human rights language and worked closely with supranational organizations, national governments and technology corporations to address problems with global disparities in quality and access — bringing rights scholars, civil society members and state officials together with representatives from ISPs, digital platforms and other private tech firms in landmark efforts to link principles of industry “self-regulation” on the Internet with human rights standards.⁷³ By the end of 1998, as the Clinton Administration handed significant managerial powers over the Internet to ICANN (essentially finalizing the privatization of the Internet), mainstream human rights scholars mostly aligned with the movement against Internet governance by national states, emphasizing instead the potential roles for NGOs, private organizations, and rights and civil liberties to play in ensuring Internet-related human rights.⁷⁴

Postel & Gilmore

Continuing the process Congress and the NSF started earlier in the decade, in 1997 the Clinton Administration published a “Framework for Global Electronic Commerce,” outlining a path forward for the government to sever its remaining ties with the technical management of the Internet for the purposes of accelerating private growth. At the time, the government estimated that it still “play[ed] a role in the operation of half the Internet’s root servers,” mostly through NSF-approved contracts with private ISPs.⁷⁵ The proposed transition would establish a private not-for-private organization (ICANN) responsible for allocating and assigning addresses in the Domain Name System (DNS) — a directory that associates Uniform Resource Locators (URLs) and email addresses with Internet Protocol (IP) addresses (e.g. <http://192.0.32.7>

translates to icann.org).⁷⁶ (Imagine trying to send a letter somewhere with roads and houses but no addresses or zip codes — the ensuing chaos might look something like an internet without a standardized DNS). Grasping the technical history of DNS management leading up to the Clinton Administration's involvement is necessary: 1) to understand the full context for the growing debate over the parameters of the privatization of the internet 2) and to find mainstream human rights theorists in relation to this historical transition.

Since 1983, Jon Postel had personally managed the Internet Assigned Numbers Authority (IANA) — serving similar functions to that which ICANN would later assume — at the University of Southern California through a contract with the U.S. Department of Defense. Postel, a poster child of the information-age luminaries (“our beloved IANA”), clashed with the DoD on multiple occasions throughout his tenure due to his opposition to the increasing concentration of power in the hands of corporations and US government officials who directly or indirectly managed the internet.⁷⁷ After the NSF authorized Network Solutions, Inc. (NSI) — the only major private domain name registration service at the time (where individuals and organizations could acquire domains) — to charge a \$50 annual fee for all domain name holders in 1995,^{78 79} Postel and many other cyber-libertarians condemned NSI's monopolistic practices. Explained one journalist:

Critics say there is no good reason why Network Solutions should have a monopoly franchise on registering the user-friendly domain names. But NSI has a great reason: By controlling the keys to prime Internet real estate, it has staked out a phenomenally lucrative business.⁸⁰

In response to widespread criticism of the new proposed fee, Postel published a working draft to institute IANA as a permanent component of DNS management in June 1996, in an effort to revoke NSI's monopoly over the system by introducing new international Top-Level Domains

(iTLDs). NSI's then-exclusive right to allocate domains under the .com, .org and .net iTLDs minimized incompatibilities between different parts of the network — ensuring interoperability, a key aspect of the cyber-libertarian vision for internet infrastructure — but interoperability, Postel argued, did not require the centralized, profit-oriented nature of NSI's function. Encouraging others to reject the privileging of NSI's exclusive TLDs, he wrote: "The inherent perceived value of being registered under a single top level domain (.COM) is undesirable and should be changed." According to Postel's draft, opening the network to new iTLDs and encouraging competition between different domain name registries would allow "competition, differentiation, and change" in Internet governance international.⁸¹

A year after Postel laid the technical and conceptual groundwork for what he and many other monopoly-wary specialists believed would be a fairer model for DNS management, John Gilmore went even further and created a new not-for-profit domain name registration service called CORE. Inspired by Postel's draft proposal for IANA and DNS, CORE's primary purpose was to compete with NSI in the hope of decreasing barriers to entry in the emerging technology.⁸² Gilmore later recounted CORE's original business model — in stark contrast to NSI's \$50 annual domain fee — stating: "It cost us less than 25 cents per year per name to run. Even if you added the likely legal bills from NSI suing us, it amounted to less than \$2 per year for each domain name."⁸³ CORE would go on to become one of the largest domain name registration services in the industry but even more immediately, Gilmore joined a chorus of other voices from across the globe criticizing the US for enabling NSI's monopoly over a core function of internet governance.

Consequences of Privatization

While many major human rights organizations and scholars coalesced around a version of Cyber-Libertarianism endorsed by Ira Magaziner and the Clinton Administration (wherein “Industry self-regulation would take the place of the Federal nanny”),⁸⁴ others in the late 90s and early 2000s identified pitfalls in an all-or-nothing position on government oversight.⁸⁵ Harvard Law Professor Jack Goldsmith for instance identified flaws in the increasingly popular movement against any and all government regulation or oversight over the Internet, or what he called “Cyberanarchy.”⁸⁶ Favoring sentiments behind the original CDA, Goldsmith suggested that “the skeptics underestimate the potential of traditional legal tools and technology to resolve the multijurisdictional regulatory problems implicated by cyberspace.”⁸⁷ This positioned Goldsmith among a minority of scholars, along with Jennifer Chang and Amy Lynne Bomse, who argued that “an overly narrow conception of government [...] reigns among Internet fans,”⁸⁸ criticising what they saw as oversimplifications underlying *Reno v. ACLU* and other hardline Cyber-Libertarian lobbies. This work resembled earlier attempts during the NWICO era to encourage states to work directly on networking technology implementation programs for the sake of protecting human rights. But debates about government oversight in the late 1990s focused primarily on questions of privacy and regulation, rather than disparities in global access, and expressions in favor of government involvement were mostly overshadowed by perceived threats over-regulation.⁸⁹

In contrast to Goldsmith’s view that “traditional legal tools and technology” could resolve the “problems implicated by cyberspace,” others argued that the Internet posed truly unfamiliar challenges for policymakers. “Analogy is the only real road map for courts when technological change leaves them in unknown legal territory,” wrote Linda Greenhouse for the

New York Times,⁹⁰ reporting on the numerous legal challenges to the CDA in early 1997.

Greenhouse depicted an ignorant judiciary system, whereby judges had to rely on analogies to TV and radio to understand the systems of infrastructure and software networks underlying the Internet — let alone regulating them. The CDA presented courts with difficult questions regarding the distinction between individual users and commercial content providers: regulations aimed at the latter threatened to apply extraneously to the former, infringing on free speech rights.⁹¹

By the end of 1997, members of the private sector, civil society groups and human rights advocates had largely defeated the government's attempts to regulate Internet content, leaning on Section 230 of the CDA — which immunized ISPs and digital platform companies from liability for content generated by individual users — to revoke the previously far-reaching regulatory power the measure granted the Federal Communications Commission's (FCC) over Internet content.⁹² Free speech advocates,⁹³ legal theorists⁹⁴ and business lawyers⁹⁵ resoundingly lauded the ruling in *Reno v. ACLU*, dubbing the amendments to the CDA a victory for First Amendment rights and a step in the right direction toward minimizing excessive legal accountability for distribution platforms for “obscene” content (and the ensuing possibilities for state censorship). Contemporary scholars point out that Section 230, or CDA 230, still stands as an epitomic representation of the US government's continuing relationship to Internet governance, defined by the protection of free speech online, by minimizing digital distributors' liabilities for user-generated content.⁹⁶

A minority of scholars concerned with the consequences of privatization continued to ring alarm bells in the early 2000s, albeit largely in vain. For example, Jennifer Chang detailed

how, in addition to repealing the ban on “indecent” speech online, *Reno v. ACLU* provided “interactive computer service” (ICS) providers⁹⁷ — including ISPs and digital platforms — with immunity “from liability for a broad array of harms arising out of information provided to the ICS by a third party.” CDA 230, argued Chang, threatened to create “a safe haven for housing discrimination” by removing ICS providers’ liability for racially discriminatory targeted advertising on their services, violating the Fair Housing Act.⁹⁸ Chang’s more critical depiction of *Reno v. ACLU* conflicted with mainstream Cyber-Libertarian narratives directly celebrating or subtextually endorsing Section 230.⁹⁹

Conclusion

By maintaining neutral stances on emerging networking technologies, leaders of the international human rights regime in the early 1990s exposed widespread uncertainty surrounding a key branch of rights theory concerning ICTs and communication rights.¹⁰⁰ A new international political order following the Cold War compounded with the recent collapse of NWICO to provide human rights scholars in the mid–late 1990s with a relatively blank slate upon which to construct new theoretical narratives about the intersection between a traditional discourse with new networking technologies.

Cornell professors Sheila Jasanoff and Dorothy Nelkin wrote for *Science* in 1982: “Too great an emphasis on the uncertainty of technological impacts can lead both scientists and regulators to recommend inaction, pending the development of better evidence of risk and causation.”¹⁰¹ With this insight, Jasanoff and Nelkin predicted the process through which

mainstream Western political theory in the post–Cold War period would transpose focus from states with ‘Communist’ regimes to instead focus on states with human rights abuses; corresponding to the development of a compatibility between foreign policy Western states on one hand, and a hybrid of Cyber-Libertarianism, a globalist human rights discourse and US First Amendment norms on the other.¹⁰²

Chapter 2 Notes

1. Boutros-Ghali, "An Agenda for Peace."
2. Jabine, Thomas B., and Richard P. Claude, eds. "Human Rights and Statistics: Getting the Record Straight." Philadelphia: University of Pennsylvania Press, 1992; Keck, Margaret E., and Kathryn Sikkink. "Human Rights Advocacy Networks in Latin America." In *Activists beyond Borders: Advocacy Networks in International Politics*, 79-120. Cornell University Press, 1998.
3. Speculation based on very few citations in published human rights scholarship using HRI in the early 1990s
4. House Committee on Science, Space and Technology. "Management of NSFNET. Hearing before the Subcommittee on Science of the Committee on Science, Space, and Technology, U.S. House of Representatives, One Hundred Second Congress, Second Session." <https://eric.ed.gov/?id=ED350986> (accessed December 10, 2018).
5. Werbach, Kevin. "Internet History: NSFNET." Cybertelecom. <http://www.cybertelecom.org/notes/nsfnet.htm#aup> (accessed December 10, 2018).
6. Office of Inspector General, National Science Foundation. "Review of NSFNET." NSF, April 23, 1993. <https://www.nsf.gov/pubs/stis1993/oig9301/oig9301.txt> (accessed December 2018).
7. Hussain, Farooq. "Historic Role Of The Commercial Internet eXchange Router And Its Impact On
8. Ogden, Jeff. "Merit Joint Technical Staff." Merit Network Inc. January 6, 1994. <https://web.archive.org/web/20110719235348/http://www.merit.edu/mail.archives/mjts/1994-01/msg00011.html> (accessed December 10, 2018).
9. African Studies Center. "About PADIS." African Studies Center, University of Pennsylvania, 2003. http://www.africa.upenn.edu/Padis/padis_ams.html (accessed November 29 2018).
10. "Supplement no. 7." In Economic and Social Council. "Economic Commission for Africa Annual Report: 29 March 1979-12 April 1980." Economic and Social Council Official Records, 1980. New York: United Nations (1980): 70.
11. Penney, Jonathon W. "Internet Access Rights: A Brief History and Intellectual Origins," *William Mitchell Law Review* 38, no. 1 (2011).
12. Carlsson, Ulla. "The Rise and Fall of NWICO." *Nordicom Review* 24 (2003).
13. Schiller, Herbert I. "Is There a United States Information Policy?" In Preston, William, Edward S. Harman, Herbert I. Schiller, Sean Macbride, Ellen Ray, and William H. Schaap. *Hope and Folly: The United States and UNESCO, 1945-1985*. University of Minnesota Press, 1989.

14. 31 Carlsson, "The Rise and Fall of NWICO."
15. Ibid., 42.
16. Movius, L. "Global Debates on the Right to Communicate." *Global Media Journal* 7, no. 13, (2008).
17. 292 Schiller, "Is There a United States Information Policy?"; 24 Carlsson, "The Rise and Fall of NWICO."
18. Shahid Akhtar, ed. *National Information and Information Policies in Africa: Report and Proceedings of a Regional Seminar Held in Addis Ababa, Ethiopia*. International Development Research Centre & Pan African Documentation and Information System. November 28 – December 1, 1988. 117, 135–136.
19. Mègnigbèto, Eustache, and Maxime Hounton. "Fortunes and Misfortunes of the CENADI in Bénin: How a National Documentation Center Disappeared." *Journal of Information Policy* 3 (2013): 59-76.
20. Ibid., 69–71
21. Ibid., 69–71
22. Kangulu, C.M., and F.E. Wood. "An Evaluation of the Pan-African Development Information System (PADIS): With Particular Reference to Zambia." *Journal of Information Science* 21, no. 5 (October 1995): 343–57.
23. Adeyah, Catherine N. "Information and Communication Technologies in Africa: A Review and Selective Annotated Bibliography: 1990-2000." International Network for the Availability of Scientific Publications, 2001. 38–38.
24. Ball, Patrick, Mark Girouard, and Audrey Chapman. "Information Technology, Information Management, and Human Rights: A Response to Metzl." *Human Rights Quarterly* 19, no. 4 (1997): 836-59.
25. Carlsson, "The Rise and Fall of NWICO."
26. Schiller, Herbert I. "Is There a United States Information Policy?"
27. Penney, "Internet Access Rights: A Brief History and Intellectual Origins."
28. Ibid., 20
29. Ball et al., "Information Technology, Information Management, and Human Rights: A Response to Metzl."
30. Crepin-Leblond, Olivier. "By Area." Internetology.
<https://nsrc.org/codes/bymap/ntlgy/bycont.htm> (accessed November 12, 2018); Dodge, Martin. "Global Internet Diffusion and Access." Geography of Cyberspace Directory.
<http://www.cybergeography-fr.org/diffusion.php> (accessed November 12, 2018); Landweber, Larry. "International Connectivity Version 9." Internet Society (August 1, 1993).
ftp://ftp.cs.wisc.edu/connectivity_table/ (accessed November 12, 2018).
31. Levy, Steven. 1984 *Hackers*. Garden City, N.Y.: Anchor Press/Doubleday.; Stallman, Richard. 1996. "MEME 2.04". Interview by David Bennahum.
<http://memex.org/meme2-04.html> (accessed November 17, 2018).

32. "A History of Protecting Freedom Where Law and Technology Collide." Electronic Frontier Foundation. <https://www.eff.org/about/history> (accessed November 12, 2018).
33. Schonfeld, Erick. "Esther Dyson On New Top-Level Domains: 'There Are Huge Trademark Issues.'" Techcrunch, July 7, 2011. <https://techcrunch.com/2011/07/21/esther-dyson-top-level-domains/> (accessed November 12, 2018).
34. Levy, Stephen. *Hackers: Heroes of the Computer Revolution*. New York: Nerraw Manijaime/Doubleday, 1984
35. Lessig, Lawrence. *Code Is Law: On Liberty in Cyberspace*. New York: Basic Books, 1999.
36. Aoki, Keith. "Considering Multiple and Overlapping Sovereignties: Liberalism, Libertarianism, National Sovereignty, 'Global' Intellectual Property, and the Internet." *Indiana Journal of Global Legal Studies* 5, no. 2 (1998): 443-73.
37. Goodman, S, Press, L, Ruth, S., and Rutkowski, A., "The Global Diffusion of the Internet: Patterns and Problems," *Communications of the ACM* 37, No 8, (August 1994): 27-31.
38. 19 Penney, "Internet Access Rights: A Brief History and Intellectual Origins."
39. Schiller, "Is There a United States Information Policy?"
40. Apodaca, Clair. "Global Economic Patterns and Personal Integrity Rights after the Cold War." *International Studies Quarterly* 45, no. 4 (2001): 587-602; Forsythe, David P. "Human Rights Fifty Years after the Universal Declaration." *Political Science and Politics* 31, no. 3 (1998): 505-11.
41. 19 Penney, "Internet Access Rights: A Brief History and Intellectual Origins."
42. Apodaca, "Global Economic Patterns and Personal Integrity Rights after the Cold War"; Blanton, Shannon Lindsey. "Foreign Policy in Transition? Human Rights, Democracy, and U.S. Arms Exports." *International Studies Quarterly* 49, no. 4 (2005): 647-67; Forsythe, "Human Rights Fifty Years after the Universal Declaration."
43. Blanton, "Foreign Policy in Transition? Human Rights, Democracy, and U.S. Arms Exports"; See also Antonio, Robert J., and Alessandro Bonanno. "A New Global Capitalism? From 'Americanism and Fordism' to 'Americanization-Globalization.'" *American Studies* 41, no. 2/3 (2000): 33-77; Ornstein, Norman J., and Mark Schmitt. "Dateline Campaign '92: Post-Cold War Politics." *Foreign Policy*, no. 79 (1990): 169-86.
44. Blanton, "Foreign Policy in Transition? Human Rights, Democracy, and U.S. Arms Exports."
45. Donnelly, Jack. "Human Rights and Foreign Policy." In *Universal Human Rights in Theory and Practice*, 197-214. Ithaca; London: Cornell University Press, 2013.
46. Clapham, Andrew. *Human Rights In The Private Sphere*. Oxford: Clarendon Press, 1993. See also Josselin, D. & W. Wallace "Non-state actors in world politics: A framework." In *Non-state Actors in World Politics*, ed. Josselin, D & W. Wallace, 1-20. Basingstoke: Palgrave, 2001; Taylor, "The Privatization of Human Rights: Illusions of Consent,

- Automation and Neutrality”; Van Ness, Peter, and Nikhil Aziz. *Debating Human Rights*. London: Routledge, 1999.
47. Donnelly, Jack. "Human Rights in the New World Order." *World Policy Journal* 9, no. 2 (1992): 249-77; Cullen, Robert. "Human Rights Quandary." *Foreign Affairs*, vol. 71, no. 5, 1992, pp. 87–88. JSTOR, JSTOR, ; Boutros-Ghali, Boutros. "An Agenda for Peace," Summit Meeting of the United Nations Security Council. Adopted January 31, 1992. In Watson, Cynthia Ann. *Stability, Security, Reconstruction, and Transition Operations: A Guide to the Issues*. Santa Barbara, CA: Praeger Security International, 2012; Tyson, Brady, and Abdul Aziz Said. "Human Rights: A Forgotten Victim of the Cold War." *Human Rights Quarterly* 15, no. 3 (1993): 589-604.
 48. United States. Congress. House Committee on Science, Space and Technology. *Management of NSFNET: Hearing before the Subcommittee on Science of the Committee on Science, Space, and Technology, U.S. House of Representatives, One Hundred Second Congress, Second Session, March 12, 1992*. Washington: U.S. G.P.O., 1992. <https://files.eric.ed.gov/fulltext/ED350986.pdf> (accessed November 18, 2018).
 49. Andjelkovic, Maja, Don MacLean, and Tony Vetter. *Internet Governance and Sustainable Development: Towards a Common Agenda*. Winnipeg: International Institute for Sustainable Development, October 2007: 29, 40–41; Bennett, Colin J. "Computers, Personal Data, and Theories of Technology: Comparative Approaches to Privacy Protection in the 1990s." *Science, Technology, & Human Values* 16, no. 1 (1991): 51-69; Boutros-Ghali, "Empowering the United Nations"; Coates, Vary T. "The Future of Information Technology." *The Annals of the American Academy of Political and Social Science* 522 (1992): 45-56.
 50. "Internet Exchange Points." Cybertelecom. March 1, 2017. <http://www.cybertelecom.org/broadband/ixp.htm#nap> (accessed December 10, 2018).
 51. National Science Foundation. "NSFNET: A Partnership for High-Speed Networking. Final Report: 1987-1995." (1995).
 52. "Jerry Berman: Founder, CDT, President and Chair, Internet Education Foundation." Center for Democracy & Technology, 2010. <https://cdt.org/about/staff/jerry-berman/> (accessed November 15, 2018).
 53. Harris, Scott. "Freedom Fighters of the Digital World." *The Los Angeles Times*, January 13, 2002. Archived at <https://web.archive.org/web/20020117210844/http://www.latimes.com:80/features/printedition/magazine/la-000003207jan13.story> (accessed November 13, 2018); Sterling, Bruce. "Conferences on the Well" in *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*. Project Gutenberg (June 19, 2008).
 54. Ball, Girouard and Chapman, "Information Technology, Information Management, and Human Rights: A Response to Metzl"; Metzl, Jamie F. "Information Technology and Human Rights." *Human Rights Quarterly* 18, no. 4 (1996): 705-46.

55. Lambert, Laura. *The Internet: A Historical Encyclopedia*. Santa Barbara: MTM Publishing (2005). 12.
56. 849 Ball et al., "Information Technology, Information Management, and Human Rights."
57. Internet Freedom Network. "First Organizational Meeting: Meeting Summary." Toronto, Canada (May 13, 1996).
https://web.archive.org/web/19970215010208/https://cdt.org/internet/960513_IFN_mtg.html
 (accessed November 16, 2018). See also United Nations Department of Economic and Social Affairs. "Chapter XIX - Privacy: Changing Boundaries." In *2001 Report on the World Social Situation*. Inclusive Social Development, 2001.
58. Barlow, John Perry. "A Declaration of the Independence of Cyberspace." Davos: The Electronic Frontier Foundation [February 8, 1996]; Dahlberg, Lincoln. "Libertarian Cyber-Utopianism and Global Digital Networks." In Hayden, Patrick. & El-Ojeili, Chamsy. *Globalization and Utopia: Critical Essays*. Basingstoke, NY: Palgrave Macmillan [2009]. 178–185; Goldsmith, "Against Cyberanarchy.")
59. Internet Freedom Network. "First Organizational Meeting: Meeting Summary"; United Nations Department of Economic and Social Affairs. "Chapter XIX - Privacy: Changing Boundaries."
60. Par. 8. Internet Freedom Network, "First Organizational Meeting: Meeting Summary."
61. Ibid., par 7.
62. Ibid., par 8.
63. Ibid., par. 9.
64. International Council on Human Rights Policy. "Journalism, Media and the Challenge of Human Rights Reporting," ICHRP. Geneva, Switzerland, 2002. 77.
65. Brenkert, "Google, Human Rights, and Moral Compromise."
66. Wallich, Paul. "Watch Your Electronic Mouth." *Scientific American* 271, no. 6 (1994): 43-44; Faucette, Jeffrey E. "The Freedom of Speech at Risk in Cyberspace: Obscenity Doctrine and a Frightened University's Censorship of Sex on the Internet." *Duke Law Journal* 44, no. 6 (1995): 1155-182; Volokh, Eugene. "Cheap Speech and What It Will Do." *The Yale Law Journal* 104, no. 7 (1995): 1805-850; Steele, Shari. "Taking a Byte Out of the First Amendment: How Free Is Speech in Cyberspace?" *Human Rights* 23, no. 2 (1996): 14-16.
67. Ball, Girouard and Chapman, "Information Technology, Information Management, and Human Rights: A Response to Metzl"; Metzl, "Information Technology and Human Rights."
68. Sorensen, Karen. "Silencing the Net: The Threat to Freedom of Expression On-line," ed. Gara LaMarche. *Human Rights Watch* 8, no. 2 (May 1996); Myers, Ken S., "Wikimmunity: Fitting the Communications Decency Act to Wikipedia." *Harvard Journal of Law and Technology*, Vol. 20, p. 163, Fall 2006; Berkman Center Research Publication No. 2006-08.

69. Myers, Ken S., "Wikimmunity: Fitting the Communications Decency Act to Wikipedia." *Harvard Journal of Law and Technology*, Vol. 20, p. 163, Fall 2006; Berkman Center Research Publication No. 2006-08. SSRN: <https://ssrn.com/abstract=916529>
70. Sorensen, "Silencing the Net: The Threat to Freedom of Expression On-line."
71. Morris, John B. Jr. "The Past, Present, and Future of Internet Censorship and Free Speech Advocacy." In *Defending the First: Commentary on First Amendment Issues and Cases*. Ed. Joseph Rossumano. Mahwah: Lawrence Erlbaum Associates (2005): 189. See also Sorensen, "Silencing the Net: The Threat to Freedom of Expression On-line."
72. Sorensen, "Silencing the Net: The Threat to Freedom of Expression On-line"; Wired News Staff. "The CDA Plaintiffs." *Wired Magazine*. June 26, 1997. <https://www.wired.com/1997/06/the-cda-plaintiffs/> (accessed November 17, 2018).
73. Machill, Dr. Marcel, Machill Jens Waltermann. "Self-regulation as a Foundation." In *Self-regulation of Internet Content*, Gütersloh: Bertelsmann Foundation (1999), 21–28.
74. Ball, Girouard and Chapman, "Information Technology, Information Management, and Human Rights: A Response to Metzl"; Metzl, "Information Technology and Human Rights"; Taylor, "The Privatization of Human Rights: Illusions of Consent, Automation and Neutrality"; Wiseberg, Laurie S. "Access to United Nations Human Rights Documentation." *Human Rights Quarterly* 19, no. 2 (1997): 350-64.
75. National Telecommunications and Information Administration. "Management of Internet Names and
76. ICANN. "What Does ICANN Do?" (2017). <https://www.icann.org/resources/pages/what-2012-02-25-en>
77. Cerf, Vint. "I Remember IANA." Network Working Group, October 17, 1998. <https://tools.ietf.org/html/rfc2468> (accessed December 10, 2018).
78. NSF. "NSF and NSI End Internet Intellectual Infrastructure Fund Portion of Domain Name Registration Fees." News Release 98-017, March 16, 1998. https://www.nsf.gov/news/news_summ.jsp?cntn_id=102875 (accessed December 10, 2018).
79. National Telecommunications and Information Administration. "Management of Internet Names and
80. Dillon, John. The Internet Is Changing from a Public Resource to a Lucrative Operation Influenced by Spooks and Former Pentagon Officials. Open Access and Information are Increasingly Controlled." *CovertAction Quarterly*.
81. Postel, Jon. "New Registries and the Delegation of International Top Level Domains." Internet Engineering Task Force, June 1996: 2. <https://tools.ietf.org/html/draft-postel-iana-itld-admin-01> (accessed December 10, 2018).
82. Cave, Damien. "It's time for ICANN to go." *Salon*, July 2, 2002. <https://web.archive.org/web/20110722170621/http://www.salon.com/technology/feature/2002/07/02/gilmore/print.html> (accessed December 10, 2018).
83. Ibid.

84. Broder, John M. "Ira Magaziner Argues for Minimal Internet Regulation." *The New York Times*, June 30, 1997. <https://nyti.ms/2nP21TE> (accessed November 12, 2018). See also Campbell, Sharon. "Youthreach: Guidelines for Writing Children's Internet Policies." *American Libraries* 29, no. 1 (1998): 91-92; The Center for Democracy and Technology. "A briefing on public policy issues affecting civil liberties online." CDT Policy Post 2, no. 7 (February 26, 1996) http://www.ciec.org/trial/cdt_pp207.html (accessed November 20, 2018); D'Haenens, Leen. "Beyond Infrastructure. Europe, The United States and Canada on the Information Highway: Where Business and Culture Collide." In *Images of Canadianness: Visions on Canada's Politics, Culture, and Economics*, ed. D'Haenens Leen, 237-54. Ottawa: University of Ottawa Press, 1998.
85. Wu, Timothy. "Application-Centered Internet Analysis." *Virginia Law Review* 85, no. 6 (1999): 1163-204. See also Chang, Jennifer C. "In Search of Fair Housing in Cyberspace: The Implications of the Communications Decency Act for Fair Housing on the Internet." *Stanford Law Review* 55, no. 3 (2002): 969-1012; Goldsmith, Jack L. "Against Cyberanarchy." *Occasional Papers from the Law School: University of Chicago*: 40.
86. Goldsmith, "Against Cyberanarchy."
87. *Ibid.*, 40
88. Bomse, Amy Lynne. "The Dependence of Cyberspace." *Duke Law Journal* 50, no. 6 (2001): 1747.
89. 1740–1750 Bomse, "The Dependence of Cyberspace"; Luke, Timothy W. "Cyberspace as Meta-Nation: The Net Effects of Online E-Publicanism." *Alternatives: Global, Local, Political* 26, no. 2 (2001): 136.
90. Greenhouse, Linda. "What Level Of Protection For Internet Speech?". *The New York Times*, 1997.
<https://archive.nytimes.com/www.nytimes.com/library/cyber/week/032497decency.html>.
91. Myers, "Wikimmunity: Fitting the Communications Decency Act to Wikipedia."; Goldsmith, "Against Cyberanarchy."
92. Myers, "Wikimmunity: Fitting the Communications Decency Act to Wikipedia."
93. Simon, Glenn E. "Cyberporn and Censorship: Constitutional Barriers to Preventing Access to Internet Pornography by Minors." *The Journal of Criminal Law and Criminology* 88, no. 3 (1998): 1015-048; Volokh, Eugene. "Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking about You." *Stanford Law Review* 52, no. 5 (2000): 1061.
94. "Developments in the Law: The Law of Cyberspace." *Harvard Law Review* 112, no. 7 (1999): 1597–1609.
95. Maloney, Marilyn C. "Intellectual Property in Cyberspace." *The Business Lawyer* 53, no. 1 (1997): 236.
96. *Harvard Law Review*. "Note: 'Section 230 As First Amendment Rule.'"; Jeong, Sarah. "A New Bill to Fight Sex Trafficking Would Destroy a Core Pillar of Internet Freedom." *The*

Verge, August 1, 2017.

<https://www.theverge.com/2017/8/1/16072680/cda-230-stop-enabling-sex-traffickers-act-liability-shield-senate-backpage> (accessed November 20, 2018). Khanna, Derek. "The Law that Gave Us the Modern Internet—and the Campaign to Kill It." *The Atlantic*, September 12, 2013.

<https://www.theatlantic.com/business/archive/2013/09/the-law-that-gave-us-the-modern-internet-and-the-campaign-to-kill-it/279588/> (accessed November 27, 2018).

97. 47 U.S.C.A. § 230(f)(2) (West 2002). In Chang, "In Search of Fair Housing in Cyberspace: The Implications of the Communications Decency Act for Fair Housing on the Internet," 972.
98. Chang, "In Search of Fair Housing in Cyberspace: The Implications of the Communications Decency Act for Fair Housing on the Internet," 1001.
99. Feingold, Russ. "attempts to prohibit indecent speech to minors on these networks raises questions of constitutionality." In 141 Cong. Rec. S8335 (June 14, 1995).
100. "Vienna Declaration and Programme of Action." World Conference on Human Rights. June 25, 1993.
101. Jasanoff, Sheila, and Dorothy Nelkin. "Science, Technology, and the Limits of Judicial Competence." *Science* 214, no. 4526 (1981): 1211-215.
102. Laudon, Kenneth C. "Markets And Privacy". *Communications Of The ACM* 39, no. 9 (1996): 92-104; Muchlinski, Peter T. "Human rights and multinationals: is there a problem?" *International Affairs* 77, no. 1 (2001). 42–43. <https://www.jstor.org/stable/2626552> (accessed November 12, 2018); Wacks, Raymond. "Are Privacy and Free Speech Possible in Cyberspace?" In *Law, Morality and the Private Domain*, 269-90. Hong Kong University Press, 2000.

Chapter 3: Private Industry, Public Square

The full text of this chapter was submitted as the final paper for a Spring 2018 tutorial with Professor Roger Berkowitz on free speech in the digital age. It should not be considered part of my Senior Project, rather it is appended here as a transition into the final chapter.

The Internet proffers a fierce battleground for academics, journalists, bloggers and vloggers debating how to conceptualize censorship and free speech in the modern era. Made up of a combination of physical networks, digital devices and virtual platforms, the Internet, on the international level, by its very nature lacks a centralized governing body to regulate traffic. Yet digital platform operators, national governments, and other groups or individuals can and do influence the laws governing how content flows — or doesn't — across digital networks. For example, representing what is probably the most expansive state censorship program in history, the “Great Firewall” Internet filtering system in China prevents nearly a fifth of the world's Internet users from accessing content deemed too critical of the government, and completely blocks websites like Facebook, Google, *The New York Times* and Wikipedia, to name a few.¹ Parallel to state-sponsored efforts to regulate information on the Internet runs an array of private companies welding complex and evolving internal policies for ‘moderating’ content on their platforms. For example, Facebook's “Community Standards” determine the acceptable forms of speech on its platform for nearly a third of the global population, with over two billion users. As

Kate Klonick argued in 2017, content moderation policies inside major American social media companies reflect a combination of adherence to traditional First Amendment discourse, “a sense of corporate responsibility,” and of course, questions of “economic viability.”² Although they are not centralized to the same extent as the Great Firewall (operationally or infrastructurally), these rules and standards comprise a system of filters similar to that in China in that they set the rules of expression and information accessibility for billions of online users. Governments and corporations thus play distinct, yet analogous roles in regulating online speech, each exercising complex and often conflicting forms of control from different points of entry into Internet traffic. How are these two forces conceptualized in free speech scholarship?

The kinds of bottlenecks Facebook and the Chinese government impose on the flow of data in different regions — due either to their relative social ubiquity, in the case of particular websites and platforms, or a tight-knit network of state-controlled Internet Exchange Points (IXPs), as in China — embody the central object of traditional free speech advocates’ gripes with the Internet. Critical scholarship focusing on one or both of these forms of Internet governance (direct censorship by states or ‘content moderation’ by digital platforms) shares foundational pillars with First Amendment doctrine from throughout history, from James Madison and John Adams to John Stuart Mill, who established core models on the theoretical significance of freedom of expression and thought in a democratic society.

Mill left few stones unturned in his landmark book *On Liberty* (1859), where the British philosopher and economist adopted and expanded significantly on the ‘harm principle’ as a means for evaluating the legitimacy of states repressing freedom of assembly, expression and information. The “freedom to unite,” he wrote, cannot be infringed on “for any purpose not

involving harm”³ — in other words, police intervention is only justified against one who causes injury to other people. Mill then included additional parameters for distinguishing between freedom and repression, based on the soundness of a person’s mind: insisting that to be repressed one must be of “full age, and not forced or deceived.”⁴ The author’s final restriction here against hindering “individual liberty” foreshadowed the challenges of defining censorship in the 21st century in response to widespread deceptive content and advertising campaigns on the Internet. In this essay I will demonstrate how scholars relying on traditional notions of censorship and free speech have constructed a environment where novel forms of manipulation are difficult if not impossible to reconcile with discursive models for addressing freedom of expression and privacy and public opinion on the Internet.

21st Century Censorship

Emerging evidence of a relatively novel form of manipulation challenges popular modern notions of how censorship and free speech work. Massive disinformation campaigns using fake accounts, fake communities, fake news and advertising on social media target the integrity of elections and democratic stability in countless nations and regions across the globe today. Rather than preventing access to or removing particular information, these subtler forms of influence overload people with falsehoods or distractions, as Yuval Noah Harari explained in 2015:

In the past, censorship worked by blocking the flow of information. In the twenty-first century, censorship works by flooding people with irrelevant information. ... In ancient times having power meant having access to data. Today having power means knowing what to ignore.⁵

Inquiries into this inverted form of censorship today increasingly contrast with historical attempts to hold social media companies accountable for their complicity with repression. Since the 2016 Presidential election, Congress has conducted at least a dozen hearings pertaining to social media companies' content moderation policies, garnering speculation that the legislature is exploring regulatory measures for reigning in the industry.⁶ But while the general public apparently shares similar concerns — a September poll found that more than half of American voters “think Facebook has too much power” — in the same survey, just 21 percent of respondents said they “want the federal government to regulate social media companies.”⁷ This discrepancy exemplifies growing conceptual rifts around the intersection between traditional free speech doctrine and 21st century censorship: while government regulation long loomed as the greatest perceived threat to free speech (especially on the Internet), today, some see it as a tempting remedy for the private sector's inflated power over freedom of expression online.

Even before 2016, academics in the US frequently delved into the policies and algorithms governing traffic on digital media platforms, as well as the related laws and norms shaping them. For examples, after Google launched a censored version of its site in China in 2006,⁸ or when Facebook banned a post by a Norwegian journalist including the iconic “napalm girl” Vietnam War photo, citing the platform's policy against child nudity.⁹ Employing traditional free speech concepts and vocabulary, critics nearly globally condemned these actions, and in both cases the companies eventually reversed their decisions: Facebook reinstated the post within 24 hours,¹⁰ and Google stopped operating its censored servers in China in 2010.¹¹ Free speech advocates have celebrated these and similar victories since the late 1990s, often denouncing prominent

institutions for abusing their power in Internet governance by removing or blocking access to particular content. But these examples pertain to more traditional forms of censorship.

Today the most prescient criticisms of the relationship between social media companies and free speech are shifting from focusing primarily on relatively cut-and-dried instances, wherein governments or corporations block information, to more novel territories, concerning repression of the nature John Stuart Mill described in 1859 against “forced or deceived” persons. Can deception influence freedom of expression on a titanic scale? Last year, the *Times* detailed the ongoing materialization of this reality, reporting that on Facebook alone, Russian disinformation campaigns designed to “sow discord among American citizens” reached 126 million users before the 2016 election. Russian influence in the 2016 President election aggravated preeminent irrationalities reigning in many factions of contemporary political discourse in US and spurred a transition in free speech scholarship to apply new and wider doctrines to the Internet. Members of the discipline are challenged with adapting a traditional discourse to relatively novel questions of accountability in mass communications.

Celebrities, journalists and politicians who cited @Ten_GOP (Tennessee Republican Party) on Twitter were embarrassed to learn that the account was fake, after the Department of Justice indicted 13 Russians involved with malicious interference in the 2016 Presidential election and cited the account as part of the incursion.¹² Twitter deleted the account in October 2017, but journalists noted that that by that time, @TN_GOP (the real Tennessee Republican Party) had already complained multiple times to the company about the fake account. In response to the first complaint in September, 2016, Twitter reportedly explained that the platform allows parodies, and therefore would not remove the account.¹³ This and similar

examples demonstrate the unfamiliar nature of the disinformation campaign, and resulting complacency on the part of platform operators. Long hailed as a bastion for free speech rights among social media companies, Twitter was forced to reevaluate its content moderation procedures in the aftermath of the 2016 election. Tennessee GOP director Michael Sullivan said after the indictments, "I really hope this is a good lesson for Twitter, social media, Facebook and YouTube."¹⁴

Twitter's future is anyone's guess, given the juxtapositions between its ideological roots and the novel issues facing social media companies today related to disinformation. In 2012, Tony Wang, then-UK general manager at Twitter, told an audience of journalists and technologists at the annual Guardian Changing Media Summit that Twitter considers itself "the free speech wing of the free speech party."¹⁵ Without a clear course of free speech terminology to deal with digital disinformation campaigns, companies enjoy relative flexibility in their public adoption of related policies and terminologies. But by the same token, they also lack effective strategies and concepts to apply in efforts to protect human rights online.

If you clicked an ad, liked a photo, or attended an event sponsored by the Russian "Internet Research Agency"¹⁶ before the election, was your vote your own, or were you coerced? Applying Robert Post's theory of "democratic competence" to Internet technologies, Stephen Vladeck outlines a helpful theoretical model for answering this question. His argument that Wikileaks should be protected by freedom of the press inversely reflects emerging discourses on obligations to remove disinformation from social media: citing Post, Vladeck argues that "the integrity (the 'competence') of public discourse"¹⁷ relies mostly or completely on "the cognitive empowerment of persons within public discourse, which in part depends on their access to

disciplinary knowledge.”¹⁸ In light of the apparent ties between digital platforms and public opinion, Vladeck applies a Postian theory of “democratic competence”¹⁹ to expose social media’s potential effects on democracy.

Post primarily argued that preserving academic freedom is crucial for maintaining some kind of “disciplinary authority that distinguishes good ideas from bad ones” in a society.²⁰ Transposing the model’s source of “authority” from academia to the Internet, Vladeck suggests that whether the process manifests in government regulation or corporate policies,²¹ the Internet today plays a crucial role in establishing norms that “distinguish good ideas from bad ones.” Conceptualizing free speech on the Internet in terms of protecting “expert knowledge,” as Post described in 2012, zooms attention out from specific cases of censorship to the broader impacts of social media companies on public opinion resulting from more invisible forms of filtering.

Private Discretion

Free speech advocates have critically examined private technology industries’ impacts on public opinion for decades. In 1999 for example, Owen Fiss described how “managerial censorship” — a form of censorship conducted by “the television industry itself” — helps to “construct the public agenda and shape public understanding.”²² While the “informal education system” in the United States consists of many components, including “films, newspapers, books, [etc.],” argued Fiss: “none is as important as television.”²³ The Internet has come to occupy an analogous role in many parts of society, with “managerial censorship” taking hold in the form of content moderation policies and filtering mechanisms at social media companies. Whereas Post sought to apply free speech principles to the academic sphere in order to protect public opinion

and the ability to distinguish “good ideas from bad ones,” Fiss undertook a theoretically a similar operation directed more discreetly at informations and communications technology industries.

In his article, “The Censorship of Television,” Fiss chronicled a history of legislation relevant not just to TV but also to contemporary discussions about the Internet. In 1969 for example, *Red Lion Broadcasting Co. v. Federal Communications Commission* established obligations for public radio stations to “use objective standards” in their broadcasting, resembling recent speculation about Congress taking action against social media companies.²⁴ In *Red Lion*, the Supreme Court “upheld FCC regulation [...] aimed at the problem of managerial censorship” by forcing “radio and television broadcasters to cover issues of public importance in a fair and balanced way.” Most importantly, Fiss argued that this and later rulings by the Supreme Court theoretically “enable[d] the suppression of some speech in the name of enhancing other speech.”²⁵ A relatively early attempt to enact content-related legislations over wireless informations and communications technologies, the ruling in *Red Lion* resembled a Postian model for regulating content moderation. Post explained, “[t]he value of democratic competence is undermined whenever the state acts to interrupt the communication of disciplinary knowledge that might inform the creation of public opinion.”²⁶ According to this account, the Supreme Court’s ruling in 1969 — demonstrating the legislature’s willingness to force broadcasters to “cover issues of public importance in a fair and balanced way”²⁷ — resembled an early version version of what Post called a “disciplinary authority.”

Later, the Supreme Court responded to the 1992 Cable Act by striking the parts of the measure granting cable operators the “authority to prohibit sexually explicit programming on leased access channels,” while upholding the authority of public access channels to do so.²⁸ The

ruling thus echoed *Red Lion* in the public sphere, but simultaneously diverged by maintaining a more absolute definition for free speech for private distributors. In his dissent, Justice Breyer voiced the opinion that would come to dominate discussions about the Internet in later years, in contrast to limited regulation over television: Fiss explained that “cable operators” in Breyer’s view, “manage a purely private communication system, and have complete discretion over what to transmit.” Over the following decade, new laws dealing with similar questions of managerial authority on the Internet came to reflect Breyer’s dissent, as part of a shift toward increasing discretionary power on the parts of Internet Service Providers. Still, as I have shown, legislation in the decades leading up to the proliferation of the Internet demonstrated attempts to regulate information and communications technology industries on the basis of the government’s authority to protect “fair and balanced” coverage.

“The New Governors”

In contrast to fifty years ago, content moderation policies today apply to singular distribution platforms where billions of people expect to be able to participate both in a “public space” and in “private spaces,” switching between the two with a simple swipe or tap.²⁹ Newer forms of censorship (not based on explicit blocking) today hinge on these platforms, and are accompanied by a wide range of moderation procedures, privacy policies and user agreements. In a detailed record of the legal foundation for tech giants’ unprecedented powers over freedom of expression and public discourse, Kate Klonick argued in 2018 that “the biggest threat this private system of governance poses to democratic culture is the loss of a fair opportunity to participate, which is compounded by the system’s lack of direct accountability to its users.”³⁰

Klonick's article, "The New Governors: The People, Rules, and Processes Governing Online Speech," details a history of how major social media companies in the US developed internal content moderation policies in relation to changing laws and norms, listing some positive, and many negative examples of the consequences of their influence over public discourse. After conducting extensive research, including interviews with current and former employees at Facebook, Twitter and Youtube, Klonick concludes: "There is very little transparency from these private platforms, making it hard to accurately assess the extent to which we should be concerned about speech regulation, censorship, and collateral censorship."

A law student, Klonick applies a more objective and arguably optimistic lens to the Internet than Owen Fiss or Robert Post, who primarily speculated on broader theoretical consequences of private content moderation rather than focusing on a comprehensive review of legislative cases related to the phenomenon. But at the core of her essay, she too pitches a radical idea. Focused on increasing opportunity and ensuring accountability related to the Internet, the author argues that mainstream scholars too often try to apply "purely First Amendment doctrine" to content moderation procedures:

Instead, platforms should be thought of as operating as the New Governors of online speech. These New Governors are part of a new triadic model of speech that sits between the state and speakers-publishers. They are private, self-regulating entities that are economically and normatively motivated to reflect the democratic culture and free speech expectations of their users.³¹

The way Klonick depicts platform companies in relation to freedom of expression here offers a new answer to Robert Post's more open-ended thinking on a "disciplinary authority that

distinguishes good ideas from bad ones,” replacing the state — as decider, in *Red Lion* and the repeal of the 1992 Cable Act for examples — with private distribution platform corporations themselves to establish standards for content filtering.³² While acknowledging the conflicting motivations inherent to the private sector, Klonick does not advocate for increased regulation. Because companies are “economically responsive to the expectations and norms of their users,”³³ she suggests that “analysis of online speech is best considered from the perspectives of private governance and self-regulation”³⁴ and therefore scholars should turn their focus to the internal policies at major companies. Through this lens, the author provides an exhaustive analysis of the history of self-regulation practices and standards in the still relatively young industry.

Ultimately Klonick settles on a somewhat contradictory prescription for future approaches to the Internet content moderation problem — but perhaps not unintentionally. She laments the “lack of accountability” in the industry while simultaneously campaigning for companies for companies to “voluntarily take up a commitment to ... [protect] individuals’ rights”³⁵ as her primary action point. “Any proposed regulation,” she wrote, “[...] should look carefully at how and why the New Governors *actually* moderate speech,”³⁶ heeding the risks of enacting legislation on impulse. This twofold approach distributes responsibility between both legislators and private actors, encouraging members of each sector to strive to understand the underlying motivations — and limitations — of the other. Klonick’s strategy in this sense symbolizes a hybrid of competing factions within human rights discourse from the previous decade by merging criticisms of states for their repression with criticisms of companies for their complicity. Without dwelling too much on past instances of censorship, Klonick paints a shared

story between two worlds equally responsible for both the repressive and democratizing powers of the Internet, providing key insight into how companies develop content moderation policies.

Klonick is among a large group of free speech advocates who emphasize Section 230 of the Communications Decency Act (CDA 230) in defense of self-regulation norms in the digital platform industry. Granting publishers and distributors on the Internet immunity from liability for content generated by 3rd-party users, Section 230 — what has been called “The Law that Gave Us the Modern Internet”³⁷ — essentially means that “online platforms can't be sued for something posted by a user [...] even if they act a little like publishers, by moderating posts or setting specific standards,” as Alina Selyukh explained.³⁸ In 1996, the CDA 230 established the regulatory flexibility for social media companies to create individual content moderation policies in the US, laying the groundwork for the rise of what Kate Klonick describes as a system of “New Governors” we see today.

Many free speech advocates today concerned with the Internet support CDA 230 and advocate for more legislation like it based on the notion that limited liability increases freedom, but others have also spoken out recently in opposition to the broad immunity it grants social media companies.³⁹ For instance, critics lamented the measure’s overinclusive terminology when it showed up late last year in a motion by the defendant to dismiss *Cockrum v. Campaign for Donald Trump*. The suit, launched by three Americans, accused the Trump Campaign of participating in “a conspiracy with Russia and WikiLeaks” to coordinate the release of emails stolen from the Clinton campaign during the election. In its motion to dismiss the case, the Trump Campaign defined CDA Section 230 and then explained:

Since WikiLeaks provided a forum for a third party (the unnamed “Russian actors”) to publish content developed by that third party (the hacked emails), it cannot be held liable for the publication.

That defeats the conspiracy claim. A conspiracy is an agreement to commit “an unlawful act.” [...] Since WikiLeaks’ posting of emails was not an unlawful act, an alleged agreement that it should publish those emails could not have been a conspiracy.⁴⁰

The motion proved successful, with a district court in DC dismissing the suit in July.⁴¹ In an indication of the lasting power of norms immunizing those involved with digital distribution from liability for content, the court explained its decision to dismiss *Cockrum*: “WikiLeaks did not subject itself to personal jurisdiction in the District simply by posting material on the Internet that could be read by District residents.”⁴² This case demonstrated CDA 230’s persisting relevance in legislation concerning Internet governance, but also it also struck a nerve among those seeking to hold digital platform companies accountable for their role in contributing to Trump’s nomination. As the attitude embodied in CDA 230 has become increasingly popular among social media companies and other defendants in ongoing investigations into Russian interference in the 2016 Presidential election, free speech and human rights scholarship are starting to show renewed concern for the potentially harmful consequences of the now 22-year old Communications Decency Act.⁴³

Amending CDA 230

Around the time when those investigating Russian interference in the 2016 election started addressing the Communications Decency Act, another key battle was unfolding between free speech advocates, legislators, members of the private sector and nongovernmental organizations over consequences of CDA 230 related to advertisements for sex trafficking on the Internet. Over the past year, a significant movement has dissented against otherwise widespread support for the Stop Enabling Sex Traffickers Act (SESTA),⁴⁴ a bill introduced in Congress last Fall primarily to hold Backpage.com accountable for hosting sex trafficking advertisements on its website.⁴⁵ SESTA slightly amends CDA 230 to clarify that “providers and users of interactive computer services” remain subject to the enforcement “of Federal and State criminal and civil law relating to sex trafficking.”⁴⁶ Joining the American Civil Liberties Union, the Center for Democracy and Technology, and the Electronic Frontier Foundation in opposition, Google public policy counsel Stewart Jeffries reportedly stated that the amendment threatens to undercut “one of the foundational statutes for the internet” by forcing companies to infringe on users’ free speech for fear of being potential liability.⁴⁷ Further illustrating the diversity of the groups opposing to the measure, the Sex Workers Outreach Project called SESTA a “disguised internet censorship bill.”⁴⁸

Opposition to SESTA demonstrates the persistence of more traditional absolutist First Amendment norms on the Internet, as its critics mostly seek to protect the immunity of digital distributors by maintaining self-regulation principles in the name of free speech. But others point out that voluntary filtering norms come with additional consequences for human rights more broadly. Taina Bien-Aimé for example, executive director of the Coalition Against Trafficking in Women, argued in support of SESTA, stating: “This is not a free speech issue, this is a crime

issue,”⁴⁹ and comedian Amy Schumer encouraged her Twitter followers to urge their representatives to support the proposed amendments to CDA 230.⁵⁰ The NGO network End Child Prostitution and Trafficking International also backed Congresswoman Ann Wagner’s (R-MO) House bill, and a “coalition including anti-trafficking advocacy groups and relatives of trafficking victims” linked to the *I am Jane Doe* movement released a letter in favor of the amendments in August 2017.⁵¹ These supporters en masse in fact resemble emerging work to revoke long-standing immunities for social media companies’ complicity with disinformation campaigns, but at least for the time being, these movements remain disconnected.

With a diverse coalition of supporters, the movement to amend CDA 230 succeeded in March, and in September a DC court dismissed an EFF-backed complaint against SESTA.⁵² Where would Kate Klonick fall in the debate over liability for sex trafficking advertisements? It is difficult to imagine that Klonick would assume a clear stance for or against the bill, and she has not published any work on it that I can find. But the author’s attachment to CDA 230 apparent in “The New Governors” suggests that she likely shares critics’ concerns about how the new amendments might upset the delicate triadic balance Klonick described between citizens, digital platforms operators and the state. Theorists with similar roots also clearly fear the bill. As recently as November, the ACLU published a letter detailing its continued opposition to SESTA.⁵³ The efforts to combat the new legislation sustain an established tradition of privileging private discretionary power in content moderation procedures, discouraging states from delving into regulation — despite the harmful consequences of enabling sex trafficking advertisements. In addition to facilitating sex trafficking as an example, Jennifer Chang also pointed out in 2002

that Section 230 created immunity for digital platforms to provide racially discriminatory housing advertisements in violation of the Fair Housing Act.⁵⁴

The tension exhibited in Klonick's groundbreaking work spans between hopes for improvements in voluntary moderation procedure on one hand, and on the other, more cynical realities suggesting that increased government regulation may be necessary to protect freedom of expression, public opinion and human rights related the Internet. With support from both political parties, the success of SESTA hints at growing momentum in Congress to regulate digital platforms — to the dismay of groups like the ACLU, the CDT and the EFF — and increasing public awareness of how social networks can hinder freedom of expression and facilitate crime. Although not yet directly linked to similar efforts concerning private sector accountability for disinformation campaigns, it is tempting to imagine that the bipartisan support for SESTA may precede more expansive regulatory systems for dealing with the impact of social media companies on freedom of expression, public opinion and democratic competence in the United States. A brief aside from the US is necessary here for understanding conversations about Internet regulation with some international context, and to bring into the mix a significant, but so far unmentioned component of the equation called 'privacy.'

The GDPR

Years ahead of the United States, the European Union enacted cohesive legislation over digital platform operators with the General Data Protections Regulation (GDPR), in effect since May 2018.⁵⁵ The extensive new regulatory structure for tackling social media comes after a series of legal battles from across Europe concerning companies' liabilities for 3rd-party content

over the past decade, most notably *Google Spain v. AEPD and Mario Costeja González*. The case represented a victory for the emerging “Right to Be Forgotten”⁵⁶ — a concept linked directly to personal user data and privacy protection on the Internet — and significantly contributed to growing pressure leading up to the implementation of the GDPR. In March 2014, European Court of Justice ruled against Google when a businessman sued the Internet search giant for refusing to remove the link to an archived news page from 1998 where an advertisement implicated the plaintiff in social security debts (both the tech company and the newspaper website had denied González’ previous requests to remove the page). The ruling in *Google Spain* suggested “that Google is not a mere processor but also a controller of personal data on third party webpages, because it is Google that decides upon the purposes and the means of the indexing activity.”⁵⁷ The decision thus directly conflicted with leading narratives in the US minimizing private sector liability for content generated by 3rd-parties on digital media platforms, upending traditional immunities for US companies operating in Europe.

Focusing heavily on “personal data,” the case remarkably emphasized companies’ obligations to respect individual control of personal information above considerations for freedom of expression, access to information and public opinion. Two years later, the European Union enacted the GDPR, a sweeping new regulatory framework through which, as *The Guardian* described in 2018, “individuals will find themselves with more power to demand companies reveal or delete the personal data they hold” and EU regulators will be able to “work in concert” to fine companies up to €20m for failing to ensure users’ control over their personal data.⁵⁸ Journalists, human rights groups and private sector interests lauded the GDPR for taking a step in the right direction toward protecting human rights related to the Internet.⁵⁹ Wrote an

online blogger for Palentir (an American software company founded by Peter Thiel): “GDPR is not a perfect solution, but it provides a good starting point for organizations to begin handling their customers’ personal data in a more ethical and responsible way.”⁶⁰ After a cumbersome 2-year implementation period, members of the industry and the human rights regime largely hailed the sweeping legislation as a major success in protecting rights online by increasing companies’ transparency and liability for the private information they process.⁶¹ In contrast to discussions about potential regulations against social media companies related to censorship or disinformation, the GDPR highlights individual proprietorship of personal data and seeks to hold digital platforms responsible for how they collect, manage and share peoples’ information.⁶²

Unlike mainstream narratives and strategies in the US for dealing with Internet governance from a First Amendment perspective, privacy-oriented legislation may enable privileging personal data rights at the expense of free speech and public information access rights. For example, a study in 2014 examined how the traditional emphasis on “personal data” in European data legislation — tracing back to the 1995 European Data Protection Directive — has enabled a handful of European nations to use regulations aimed at protecting privacy to infringe on free speech and freedom of the press.⁶³ As the ruling in *Google v. AEDP* has expanded to protect the “Right to Be Forgotten” in more standardized language across the entire EU, many scholars have harshly criticized the movement, expanding on the 2014 study to argue against new regulations. For instance, in an analysis of the recently-announced GDPR in 2015, Daphne Keller wrote: “the GDPR tilts the playing field powerfully in favor of privacy rights — and incentivizes widespread deletion of online expression even in cases where no privacy or data protection right is really infringed.”⁶⁴ Keller and others thus identified an unhealthy balance

between free speech and other more novel rights on the Internet in the EU in the years leading up to the implementation of the GDPR. These ongoing debates in Europe set the scene for similarly contentious battles in the US over whether privacy-focused legislation can be enacted without threatening the First Amendment.

The GDPR came to the forefront of public attention in the United States as companies from around the world updated their privacy policies and data management procedures to meet the new regulations in the month leading up to May 2018, when the EU began fully enforcing the measures.⁶⁵ Immediately after the law took effect, a number of websites and other Internet services in the US blocked access in Europe to avoid incurring fines, rather than updating their policies and procedures, and scholars were quick to express concerns that the GDPR could have unintended consequences for free speech on the Internet even outside of the EU.⁶⁶ Although some in the US have moved recently to replicate aspects of the new legislative model in Europe — for instance, in April Senators Amy Klobuchar and John Kennedy introduced the Social Media Privacy and Consumer Rights Act, seeking to grant the Federal Trade Commission authority to enforce citizens' control over their online data⁶⁷ — free speech advocates have largely balked at these attempts, in defense of more traditional strategies to protect free speech through broad immunities for digital distributors.

Amplifying Kate Klonick's support for CDA 230, many scholars in the US reject proposals to establish domestic regulations to replicate the GDPR. While the Center for Democracy and Technology (an opponent of SESTA) endorsed the European model for regulating online privacy,⁶⁸ members of the Electronic Frontier Foundation warned that it could be "misused to censor speech" in 2015.⁶⁹ As in the EFF's complaint, other arguments against the

GDPR in the US often identify potential threats the privacy model poses to the “balance” between “the privacy claim” versus “public interest considerations such as freedom of expression.”⁷⁰ Debates over privacy regulations like the GDPR are thus founded on an inverse conceptual relationship between privacy and freedom of expression on the Internet. In fact, as we have seen this conceptual balance underpins scholarship focusing both on privacy and on censorship, wherein observers either criticize privacy regulations for hindering free speech or criticize legal immunities for harming personal privacy rights.

Privacy vs. Censorship: A Flawed Paradigm

Thus far I have explored one basic question, plus three subsequent answers or trends in contemporary discourse, regarding private obligations to uphold free speech and human rights on the Internet. How should we conceptualize free speech and censorship in the 21st century? The first model or framework for answering this question, most popular before 2016, is characterized by an emphasis on traditional forms of censorship, in which governments or corporations directly block access to particular information. An entire essay could be devoted to filtering related to the “Community Standards” pages on Facebook alone (and many are), often with dramatic implications for activists on both sides of the political spectrum — including growing criticisms aimed at social media companies for ‘politically biased’ filtering. Similarly, the “Great Firewall” is the subject of a number of books and publications covering the regime’s vast impacts on freedom of speech and access to information in China over the past decade.⁷¹ These examples merely scratch the surface of Internet censorship, but crucially highlight the different types of actors involved with filtering or removing online content. For now it suffices to say that this

category of scholarship is primarily driven by identifying traditional forms of censorship — without necessarily making a significant distinction between private or public actors, but rather reflecting on their shared accountability for infringing on freedom of expression.

Kate Klonick embodies the second trend in my model, somewhat similar to the first but with a more concrete answer to the question of how to assign disciplinary authority in regulating content moderation procedures. With an exhaustive review of the history of moderation policies at social media companies and related laws, Klonick suggests that popular digital platforms should be considered on the same level as states and citizens in their power over freedom of speech. While open to more government involvement, she urges legislators to heed the standing powers of Facebook, Twitter, Youtube and other major social media platforms in the US before enacting new legislation. Owen Fiss and Robert Post help contextualize Klonick's theory of the "New Governors" with somewhat broader analyses of the relationships between private actors and freedom of speech in history. In her article, Klonick applies an argument similar to Post's theory of "democratic competence" to expound the influence of digital platform operators over freedom of expression. But while she alludes to other contemporary issues related to disinformation and 'election hacking,' Klonick avoids this path altogether in her work.

Still predominantly based on a traditional notion of censorship, the GDPR and other privacy-related regulations denote a third distinct category of contemporary scholarship. For nearly a decade, arguments both for and against privacy regulations in the European Union have hinged on the balance between personal data rights and freedom of expression. Simply put, members of the EU as a result today enjoy much better legal protections than US citizens for controlling their data online — but at a (debatably) high risk to freedom of information. Platform

companies in the US on the other hand have long operated with broad immunities for user-generated content and complete discretion over their moderation procedures, thanks to CDA 230 and a strong lobby from free speech advocates and the private sector. Since the early 2000s, scholars have pointed out the harmful consequences of an unfettered Internet industry — from racially discriminatory housing lists to advertisements for sex trafficking — but private power in the industry has only grown, especially with regard to free speech issues. Widespread support for SESTA over the past year demonstrated some will to revoke aspects of the immunities granted by CDA 230, but the timing on legislation aimed at blocking sex trafficking advertisements does not bode well for the condition of the overall movement to protect related non-free-speech rights online. Furthermore prominent groups like the ACLU and powerful private interests continue to oppose any legislation that they claim threaten the free speech principles underlying CDA 230, indicating a diverse coalition of opponents facing anyone seeking to hold digital platform operators more accountable for the content they provide in American context today.

After all this there remains an elephant in the room: disinformation. Where would, say, the Russian influence campaign on the 2016 US Presidential election factor in relation to the conceptual frameworks described above? It is not immediately obvious that free speech and disinformation are even necessarily related: as Yuval Noah Harari explained, the two depend on nearly opposite occurrences (information blocking vs. information overload). Free speech advocates both in the US and abroad focusing on privacy or more traditional forms of censorship have generally defined information manipulation primarily in terms of blocking access and denying transparency. But reading Klonick through a Postian lens reveals a key link between the powers of the “New Governors” to filter and the powers of individuals or groups to exploit those

filters for nefarious purposes: both directly impact freedom of expression, and perhaps more broadly can influence public opinion.

Dominant contemporary narratives concerning the Internet among free speech and human rights advocates today collectively presuppose a paradigm, hinging on traditional forms of information control, between privacy rights and freedom of expression.⁷² Although both bodies of scholarship are heavily influenced by private interests, members of each in recent years have successfully pushed for increasing regulations to control filtering techniques and forcing digital platform operations to protect users' control over personal information. In October the Information Commissioner's Office, a UK digital privacy watchdog, fined Facebook £500,000 for illegal breaches in 2015 linked to the data firm Cambridge Analytica — the maximum possible fine applicable before the GDPR went into effect. Many argued that the penalty was too low,⁷³ however just this week the Italian Competition Authority fined the company \$11,400,000 for “using people's data for commercial purposes in ways that break the country's laws” in charges unrelated to the GDPR.⁷⁴ I personally celebrate these and similar penalties levied against social media companies, but I also note the persisting disconnect between regulation focusing on privacy issues and a growing public focus on disinformation and subtle manipulation campaigns. It seems that the discursive lens of free speech has brought me in somewhat of a circle.

Thankfully Post can help break us out of this circle. In 2018, he deconstructed the problem underlying mainstream privacy regulation movements in Europe and in the US, writing: “if we imagine a social world that does not consist of persons struggling against large, impervious bureaucratic organizations, but instead of individuals engaged in continuous dialogue [...] ‘control’ is simply the wrong metaphor to apply.”⁷⁵ This keen observation applies to a vast

majority of the works discussed thus far in my essay. The categories of scholarship listed above — anti-regulation; pro-private-regulation, anti-state-regulation; and pro-state-regulation, anti-private-regulation — are each based on the notion that information control occurs through platform moderation. Or more simply, as Post describes, they are based on the metaphor of “control.” Quoting the European Commission, Post illustrates how proponents of the GDPR underestimate the underlying conflict between privacy and freedom of expression:

When pressed, reconciliation is explained through the metaphor of striking “a balance between [data] privacy and freedom of expression.” But it is hard to understand how the image of balancing makes sense when data privacy and freedom of expression presuppose mutually exclusive social domains.⁷⁶

In his conclusion the author harshly criticizes the terminological ambiguity of the “Right to Be Forgotten,” and the risks associated with *Google Spain* and the GDPR. Like Klonick, Post concedes that “[t]here is room for suspicion about how influential actors like Facebook seek to shape the development of [privacy] norms.” This subject in fact symbolizes the central point of inquiry in Klonick’s work. Expanding, Post assumes an ultimate position similar to that of Klonick when he additionally points out the powerful role digital platforms have come to occupy in democratic structures, writing: “But this suspicion ought not to blind us to the emergence of a virtual public sphere that is of enormous contemporary significance and that is sustained by an infrastructure of search engines like Google.”⁷⁷ If we accept the idea that social media companies today represent the phenomenon through which “[t]hose who control the circulation of personal data in the public sphere control the creation of public opinion,”⁷⁸ it becomes necessary to

concede the inevitability of social media's impacts not just on filtering and censorship, but on the very definition of freedom of expression in a society and public discourse more broadly.

Post offers no alternative for the “control” metaphor, so I propose moving forward by transitioning to a metaphor of ‘influence.’ As I have shown in this essay, various branches of free speech and human rights scholarship have focused on competing forms of control over Internet governance in the past two decades. These discussions fundamentally focus either on privacy rights or on traditional forms of free speech, and repeatedly revert to conceptual debates over the indefinite struggle between these two ideals. With the help of a Postian theory of “democratic competence,” moving away from the control metaphor opens up the conversation about free speech to additional forms of manipulation on the Internet. The influence metaphor is useful both because it indicates a less direct form of control over the laws dictating Internet governance and because it points to the broader effects of the phenomenon further down the chain of impact, such as has been dubbed ‘election hacking.’

In light of ongoing revelations concerning novel forms of manipulation on the Internet, I turn to Jiang Ying, who made much of the same argument I have in this paper in his 2012 book, *Cyber-Nationalism in China: Challenging Western Media Portrayals of Internet Censorship in China*. A lengthy excerpt is helpful here for highlighting how acutely Ying foreshadowed contemporary scholarship in Europe and the US concerning the increasingly-apt influence metaphor for describing Internet governance:

Traditionally, censorship was regarded as a state procedure to protect its own power over what went on in the public sphere, usually “a set of concrete measures

carried out by someone in a position of authority” (Muller 2004, p. 4). Under this conception, the state directly exercised censorial power over subjects (Post 1998). However, recent research describes censorship as an effect rather than a feature of power: it can form society in unforeseen ways even when it may also deprive subjects of freedoms such as access to public discussion (see Butler 1997).⁷⁹

Writing in 2012, Ying’s analysis far outpaced that of Western scholars in identifying the subtler forms of control embedded in the Internet, essentially completing the operation of tying Vladeck’s reading of Post to Klonick’s theory as I have done here. Ying does so however with a more pointed criticism and from an outsider’s perspective on Western portrayals of Internet censorship in China specifically. His viewpoint helps to conclude this essay with a concise review of the phenomenon I less elegantly attempted to illustrate in the preceding pages.

Traditional free speech scholarship, and its interplay with work concerning other rights on the Internet, as we have seen, lacks the capacity to address novel problems facing freedom of expression and public opinion stemming from digital disinformation campaigns. Ying’s critique of Western conceptions of censorship suggests that Russian influence merely co-opted an already well-established arm of the governance structures shaping public opinion in the US, largely unidentified in mainstream free speech scholarship. Explained Ying: “In the seemingly most transparent democratic regimes [...] governments seek to foster self-regulation as their dominant technology of governance.”⁸⁰ Thus in privileging traditional forms of regulatory censorship by states and corporations, free speech and human rights scholars have complied with the gradual privatization of public spaces and the private sector’s adoption of First Amendment authority. This essay demonstrates how omitting criticisms of susceptibility to disinformation campaigns

on the Internet unwittingly welcomes the phenomenon. The question of how social media companies profit from ‘bad actors’ influencing public opinion through their platforms remains unanswered, and I also have yet to explore an alternative framework for discussing free speech and censorship in the 21st century at length. I will discuss these and other topics in the next and final chapter.

Chapter 3 Notes

1. Fu, Furio. "The List Of Blocked Websites In China In 2018 - Latest News." *Sapore Di Cina*, September 18, 2018.
<https://www.saporedicina.com/english/list-of-blocked-websites-in-china/> (accessed December 7, 2018). See also Statista. "Number Of Internet Users Worldwide 2005-2017." The Statistics Portal.
<https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/> (accessed December 7, 2018); Rauhala, Emily. "America Wants to Believe China Can't Innovate. Tech Tells a Different Story." *The Washington Post*, July 19, 2016.
http://wapo.st/29LyC2N?tid=ss_tw&utm_term=.74cca09e64bb (accessed December 7, 2018).
2. Klonick, Kate. "The New Governors: The People, Rules, and Processes Governing Online Speech." *Harvard Law Review* 131, no. 6 (April 2018): 1598.
<https://ssrn.com/abstract=2937985> (accessed December 7, 2018).
3. Mill, John Stuart. *On Liberty*. Kitchener, Ontario: Batoche Books Limited, 2001.
4. *Ibid.*, 16.
5. Yuval Noah Harari, *Homo Deus: A Brief History of Tomorrow*. Quoted in Zizek, Slavoj. *Incontinence of the Void: Economico-Philosophical Spandrels*. Cambridge: The MIT Press (2017): 132.
6. McCabe, David. "Scoop: 20 Ways Democrats Could Crack Down On Big Tech." *Axios*, July 30, 2018.
<https://www.axios.com/mark-warner-google-facebook-regulation-policy-paper-023d4a52-2b25-4e44-a87c-945e73c637fa.html> (accessed December 7, 2018)
7. Rasmussen, Scott. "55% Believe Facebook Has Too Much Power." *Scottrasmussen.com*, September 10, 2018. <https://scottrasmussen.com/55-believe-facebook-has-too-much-power/> (accessed December 7, 2018).
8. MacKinnon, Rebecca. "How Multinational Internet Companies assist Government Censorship in China." In "Race to the Bottom" Corporate Complicity in Chinese Internet Censorship." *Human Rights Watch* 18, no. 8(C) (August 2006).
<https://www.hrw.org/reports/2006/china0806/5.htm> (accessed December 7, 2018).
9. Levin, Sam, Julia Wong, and Luke Harding. "Facebook Backs Down From 'Napalm Girl' Censorship And Reinstates Photo." *The Guardian*, September 9, 2016.
<https://gu.com/p/52b2j/stw> (accessed December 7, 2018).
10. Abutaleb, Yasmeeen and Terje Solsvik. "Facebook Reinstates Vietnam Photo After Outcry Over Censorship." *Reuters*, September 9, 2018. <http://reut.rs/2coGNab> (accessed December 7, 2018),
11. Carlson, Nicholas "Google Pulls Search Engine Out Of China." *Business Insider*, March 22, 2010. <https://www.businessinsider.com/google-pulls-out-of-china-2010-3> (accessed December 7, 2018).
12. Martinelli, Marisa. "How Did an Itty-Bitty Piece of Russian Propaganda Wind Up in Slate?" *Slate*.
13. Torrez, James. "Tennessee GOP Says They Tried To Report '@TEN_GOP' Before DOJ Indictments." *News Channel 9 WTVC*, February 16, 2018.

- https://newschannel9.com/news/local/tennessee-gop-says-they-tried-to-report-ten_gop-before-doj-indictments (accessed December 8 2018).
14. Torrez, "Tennessee GOP Says They Tried To Report '@TEN_GOP' Before DOJ Indictments."
 15. Halliday, Josh. "Twitter's Tony Wang: 'We Are The Free Speech Wing Of The Free Speech Party.'" *The Guardian*, March 22, 2012. <https://gu.com/p/36ceb/stw> (accessed December 8 2018).
 16. Chen, Adrian. "The Agency." *The New York Times*, June 2, 2015. <https://www.nytimes.com/2015/06/07/magazine/the-agency.html> (accessed December 10 2018).
 17. Vladeck, Stephen I. "Democratic Competence, Constitutional Disorder, and the Freedom of the Press." *Washington Law Review* 87 (2012) <http://digital.law.washington.edu/dspace-law/bitstream/handle/1773.1/1141/87WLR0529.pdf> (accessed December 7, 2018).
 18. *Ibid.*, 540.
 19. *Ibid.*, 532.
 20. Post, Robert. C "Democracy, Expertise and Academic Freedom: a First Amendment Jurisprudence for the Modern State," (2012). In 532 Vladeck, "Democratic Competence, Constitutional Disorder, and the Freedom of the Press."
 21. *Ibid.*
 22. Fiss, Owen. "The Censorship of Television." In Bollinger, Lee C., and Geoffrey R. Stone. *Eternally Vigilant: Free Speech in the Modern Era*. Chicago: University of Chicago Press, 2002.
 23. *Ibid.*, 262.
 24. *Red Lion Broadcasting Co. v. Federal Communications Commission*, 395 U.S. 367 (1969).
 25. 274 Fiss, "The Censorship of Television."
 26. Post, Robert. C "Democracy, Expertise and Academic Freedom: a First Amendment Jurisprudence for the Modern State." In 532 Vladeck, "Democratic Competence, Constitutional Disorder, and the Freedom of the Press."
 27. 274 Fiss, "The Censorship of Television."
 28. *Ibid.*, 268.
 29. Camp, Jean and Y.T. Chien. "The Internet as Public Space: Concepts, Issues, and Implications in Public Policy." *ACM SIGCAS Computers and Society* 30, no. 13 (September 2000). https://sites.hks.harvard.edu/m-rcbg/research/j.camp_acm.computer_internet.as.public.space.pdf (accessed December 7, 2018).
 30. Klonick, "The New Governors: The People, Rules, and Processes Governing Online Speech."
 31. *Ibid.*, 1603.
 32. Post, Robert. C "Democracy, Expertise and Academic Freedom: a First Amendment Jurisprudence for the Modern State." In 532 Vladeck, "Democratic Competence, Constitutional Disorder, and the Freedom of the Press."
 33. 1664 Klonick, "The New Governors: The People, Rules, and Processes Governing Online Speech."
 34. *Ibid.*, 1662.

35. Ibid., 1668.
36. Ibid., 1670.
37. Khanna, Derek. "The Law That Gave Us The Modern Internet—And The Campaign To Kill It." *The Atlantic*, September 12, 2013.
<https://www.theatlantic.com/business/archive/2013/09/the-law-that-gave-us-the-modern-internet-and-the-campaign-to-kill-it/279588/> (accessed December 7, 2018).
38. Selyukh, Alina. "Section 230: A Key Legal Shield For Facebook, Google Is About To Change." *All Tech Considered*. Npr.org, March 21, 2018. <https://n.pr/2G3P5QF> (accessed December 7, 2018).
39. Khanna, "The Law That Gave Us The Modern Internet—And The Campaign To Kill It"; Reslan, Ziad. "It's Time for Facebook and Twitter to Coordinate Efforts on Hate Speech." *Techcrunch*, September 1, 2018. <https://tcrn.ch/2ox6eu4> (accessed December 7, 2018.); Weissman, Cale Guthrie. "Ted Cruz Made it Clear He Supports Repealing Tech Platforms' Safe Harbor." *Fast Company*, October 17, 2018. <https://www.fastcompany.com/90252598/> (accessed December 7, 2018).
40. Justia. *Cockrum Et Al v. Donald J. Trump for President, Inc. Et Al*. (12 July 2017): 12. <https://www.politico.com/f/?id=0000015f-5581-d77a-a35f-f5e9ab300001> (accessed December 7, 2018).
41. Ibid.
42. Ibid., 36.
43. Gellis, Cathy. "Trump Campaign Tries To Defend Itself With Section 230, Manages To Potentially Make Things Worse For Itself." *Techdirt*, October 27, 2017. <https://www.techdirt.com/articles/20171027/06132038496/> (accessed December 7, 2018); Yim, Joshua. "Section 230 and Fake News." *Northwestern University Law Review Online*, April 12, 2018. <http://blog.northwesternlaw.review/?p=868> (accessed December 7, 2018).
44. Mucha, Sarah. "Senate Approves Anti-Sex-Trafficking Bill." *CNN*, March 21, 2018. <https://www.cnn.com/2018/03/21/politics/sex-trafficking-bill/index.html> (accessed December 7, 2018).
45. Llanso, Emma and Sasha Moss. "Frequently Asked Questions: Section 230, Sex Trafficking, and Current Legislation." *CDT.org*, January 22, 2018. <https://cdt.org/insight/frequently-asked-questions-section-230-sex-trafficking-and-current-legislation/> accessed Decmber 7, 2018); Portman, Rob. "Holding Backpage.com Accountable." *The Blade*, August 20, 2017. <https://www.toledoblade.com/Op-Ed-Columns/2017/08/20/Holding-Backpage-com-accountable.html> (accessed December 7, 2018); Solon, Olivia, and Sabrina Siddiqui. "Why Is Silicon Valley Fighting A Sex Trafficking Bill?" *The Guardian*, September 7, 2017). <https://gu.com/p/744f2/stw> (accessed December 7 2018).
46. S.1693, 115th Cong., *Congress.gov* (2018) (enacted). <https://www.congress.gov/bill/115th-congress/senate-bill/1693/text> (accessed December 7, 2018).
47. Jeffries, Stewart. In Solon and Siddiqui, "Why Is Silicon Valley Fighting A Sex Trafficking Bill?"
48. Andrews, Alex. "SWOP-USA Stands in Opposition of Disguised Internet Censorship Bill SESTA, S. 1963." *Sex Workers Outreach Project-USA*, August 11, 2017. <http://www.new.swopusa.org/2017/08/11/call-to-actionpress-release-swop-usa-stands-in-dire>

- ct-opposition-of-disguised-internet-censorship-bill-sesta-s-1963-call-your-state-representatives-and-tell-them-to-fight/ (accessed December 7, 2018).
49. Bien-Aimé, Taina. In Solon and Siddiqui, "Why Is Silicon Valley Fighting A Sex Trafficking Bill?"
 50. Schumer, Amy. Twitter Post. September 6, 2017, 4:31 pm. <https://twitter.com/amyschumer/status/905574257018712066>
 51. Jeong, Sarah. "Sex Trafficking Bill is Turning into a Proxy War Over Google." *The Verge*, September 14, 2017.
 52. *Woodhull Freedom Foundation et al. v. USA* (District Of Columbia District Court September 24, 2018). <https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=2813&context=historical> (accessed December 7, 2018).
 53. ACLU to Senate Commerce committee, November 7, 2017. <https://www.aclu.org/letter/aclu-letter-opposing-sesta> (accessed December 7, 2018).
 54. Chang, Jennifer C. "In Search of Fair Housing in Cyberspace: The Implications of the Communications Decency Act for Fair Housing on the Internet." *Stanford Law Review* 55, no. 3 (2002): 969-1012. doi:10.2307/1229678.
 55. *General Data Protection Regulation*. European Union (2016/679). <https://gdpr-info.eu/> (accessed December 7, 2018).
 56. Houser, Kimberly A. and W. Gregory Voss. "GDPR: The End of Google and Facebook or a New Paradigm in Data Privacy?" *Journal of Law & Tech.* no. 1 (2018).
 57. Van Eecke, Patrick. "ECJ rules 'right to be forgotten' applies to search engines." International Association of Private Professors, May 13, 2014. <https://iapp.org/news/a/ecj-rules-right-to-be-forgotten-applies-to-search-engines/> (accessed December 7, 2018).
 58. Hern, Alex. "What Is GDPR And How Will It Affect You?" *The Guardian*, May 21, 2018. <https://gu.com/p/8cnzg/stw> (accessed December 8 2018).
 59. "The EU General Data Protection Regulation: Questions and Answers." Human Rights Watch, June 6, 2018. <https://www.hrw.org/news/2018/06/06/eu-general-data-protection-regulation#> (accessed December 7, 2018); Demet, George. "The GDPR and Data Privacy as a Human Right." Palantir.net Blog, April 25, 2018. <https://www.palantir.net/blog/gdpr-and-data-privacy-human-right> (accessed December 7, 2018).
 60. Demet, "The GDPR and Data Privacy as a Human Right."
 61. "The EU General Data Protection Regulation: Questions and Answers." Human Rights Watch; "APC Welcomes the EU's General Data Protection Regulation, Calls for Stronger Privacy Protections Globally." Association for Progressive Communications, May 2018. <https://www.apc.org/en/pubs/apc-welcomes-eus-general-data-protection-regulation-calls-stronger-privacy-protections-globally> (accessed December 7, 2018); Minović, Adriana. "GDPR: Integrating Human Rights into Business Practices." DipliFoundation, November 13, 2017. <https://www.diplomacy.edu/blog/gdpr-integrating-human-rights-business-practices> (accessed December 7, 2018).
 62. *General Data Protection Regulation*. European Union (2016/679).

63. Erdos, David. "Fundamentally Off Balance: European Union Data Protection Law And Media Expression." *University of Cambridge Faculty of Law Research Paper* no. 42 (July 25, 2014). SSRN Electronic Journal. doi:10.2139/ssrn.2471531.
64. Keller, Daphne. "Free Expression Gaps In The General Data Protection Regulation." The Center for Internet and Society, November 30, 2015. <http://cyberlaw.stanford.edu/blog/2015/11/free-expression-gaps-general-data-protection-regulation> (accessed December 8 2018).
65. Fung, Brian. "Why You're Getting Flooded with Privacy Notifications in Your Email." *The Washington Post*, May 25, 2018. <https://wapo.st/2kp0eBt> (accessed December 7, 2018).
66. Wimmer, Kurt. "Free Expression And EU Privacy Regulation: Can The GDPR Reach U.S. Publishers?" *Syracuse Law Review* 68 (June 2018). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3188974. (accessed December 7, 2018); Ariès, Quentin, Tony Romm and James McAuley. "As Europe's Data Law Takes Effect, Watchdogs Go After Tech Companies." *The Washington Post*, May 25, 2018. <https://wapo.st/2IJRNPK> (accessed December 7, 2018).
67. Sandler, Alyson. "Senators Klobuchar and Kennedy Introduce Privacy Legislation." *Inside Privacy*, April 25, 2018. <https://www.insideprivacy.com/united-states/congress/senators-klobuchar-and-kennedy-introduce-privacy-legislation/> (accessed December 7, 2018); Pitman, Jamie. "Is GDPR Coming to the USA?" *Brightlocal*, August 2, 2018. <https://www.brightlocal.com/2018/08/02/is-gdpr-coming-to-the-usa/> (accessed December 7, 2018).
68. O'Connor, Nuala. "GDPR is an Important Advance in Privacy. Here's What Must Come Next." *CDT.org*. May 25, 2018. <https://cdt.org/blog/gdpr-is-an-important-advance-in-privacy-heres-what-must-come-next/>
69. Akturk, Aylin and Jeremy Malcolm. "Unintended Consequences, European-Style: How the New EU Data Protection Regulation will be Misused to Censor Speech." *Electronic Frontier Foundation*, November 20, 2015. <https://www.eff.org/deeplinks/2015/11/unintended-consequences-european-style-how-new-eu-data-protection-regulation-will> (accessed December 7, 2018).
70. Par. 10 Akturk and Malcolm, "Unintended Consequences, European-Style: How the New EU Data Protection Regulation will be Misused to Censor Speech."
71. Jiang, Ying. "Chinese Anger at the Label of Censorship." In *Cyber-Nationalism in China: Challenging Western Media Portrayals of Internet Censorship in China*, 63-76. South Australia: University of Adelaide Press, 2012. <http://www.jstor.org/stable/10.20851/j.ctt1sq5x62.9>.
72. Post, Robert. C. "Data Privacy and Dignitary Privacy: Google Spain, the Right to Be Forgotten, and the Construction of the Public Sphere." *Yale Law School, Public Law Research Paper No. 598* (April 2017). <https://ssrn.com/abstract=2953468> (accessed December 7, 2018).
73. Vincent, James. "UK data watchdog fines Facebook maximum legal amount for Cambridge Analytica scandal." *The Verge*, October 25, 2018. <https://www.theverge.com/2018/10/25/18021900/facebook-cambridge-analytica-scandal-uk-data-watchdog-ico-fines-maximum-amount> (accessed December 8, 2018).; Osborne, Charlie. "Facebook could face \$1.63bn fine under GDPR over latest data breach." *ZDNet.com*,

October 2, 2018.

<https://www.zdnet.com/article/facebook-could-face-billions-in-fines-under-gdpr-over-latest-data-breach/> (accessed December 9, 2018).

74. Collins, Katie. "Facebook fined \$11.4M in Italy over data misuse." CNet, December 7, 2018. <https://www.cnet.com/news/facebook-fined-11-4m-in-italy-over-data-misuse/> (accessed December 8, 2018).
75. 24 Post, "Data Privacy and Dignitary Privacy: Google Spain, the Right to Be Forgotten, and the Construction of the Public Sphere."
76. *Ibid.*, 27.
77. *Ibid.*, 101.
78. *Ibid.*, 80.
79. 68 Jiang, Ying. "Chinese Anger at the Label of Censorship."
80. *Ibid.*, 74.

Chapter 4: The Internet and the Ideological State Apparatus

Today more than ever before in recent history, the promises of an international human rights regime, emboldened by liberalism and globalist ideals, are in peril, as right-wing populist candidates establish a dominant foothold on new digital battlegrounds. The First Amendment, a legal tool long associated with progressive politics, has been transformed into a weapon of the alt-right, where Steve Bannon, Alex Jones and other radically xenophobic nationalists have moved from the fringe to the front page by disguising hatred, paranoia and racism as free speech. All the data-crunching software in the arsenal of left has proven futile against a new wave of fascist political leaders and ideologies sweeping across not just the United States but the entire globe, and those who celebrated Obama's successes on social media in 2008 and 2012 are left wondering where it all went wrong. It appears that the tables have turned beneath the noses of the technophiles.

Since Donald Trump's ascension to the White House, social media companies have come under intense scrutiny for the role they played in propagating a multiplex Russian influence campaign aimed at sowing social and political division within the United States. More broadly, a slew of data breaches and hacking scandals over the past two years have turned a public spotlight onto the proprietors of tech giants like Facebook, as everyday Americans start to wake up to the wide-ranging and unfamiliar dangers inherent to an unfettered conglomeration of privately-owned digital platforms claiming to provide a neutral medium for public discourse and open debate. Although social media companies have been the subject of intense scrutiny for complicity in government censorship and other infringements on human rights in the past, these

new developments in the last three years have invigorated a movement with unprecedented support to comprehend and to reign in these inflated powers. This year, for the first time since its founding, the percentage of Americans on Facebook fell, from eighty percent to seventy-seven percent.¹

Whereas in the past, digital platform operators have often successfully employed positive narratives about the interplay between social media and freedom of speech in the international context, leaders in industry now spend nearly as much time apologizing for their companies as they once spent self-congratulating. After Cambridge Analytica ex-employee and whistleblower Christopher Whaley exposed the British consulting firm in March 2018 for secretly harvesting data from 87 million Facebook accounts — and using that information to influence the 2016 U.S. elections, as well as the Brexit referendum — Facebook founder and CEO Mark Zuckerberg published a full-page advertisement in major newspapers in both countries, an apology letter promising to take steps “to ensure this doesn't happen again.”² And in a Congressional hearing in April, Zuckerberg said, “It was my mistake, and I’m sorry. I started Facebook, I run it, and I’m responsible for what happens here.”³

As more evidence continues to surface implicating foreign powers and ‘bad actors’ in the rise of fascist political ideologies domestically, little to no precedent exists for asking what responsibility digital distribution platforms have in the ongoing crisis. Presenting free speech advocates with novel challenges, disinformation campaigns demand paradigm shifts in traditional scholarship that has long been based around instances where governments or corporations block access to particular content. At this point let us introduce our last major

theorist relevant to my project, a Marxist philosopher whom I believe all aspiring college professors should be required to read.

In 1971 Louis Althusser postulated that alongside its own direct, repressive means, the state also constantly asserts its power and reinforces the dominant bourgeois ideology through Ideological State Apparatuses (ISAs). These systems are comprised by private and public organizations alike, each with unique forms of influence over public discourse and sociopolitical norms. They include:

1. The Scholastic Apparatus
2. The Familial Apparatus
3. The Religious Apparatus
4. The Political Apparatus
5. The Associative Apparatus
6. The Information and News Apparatus
7. The Publishing and Distribution Apparatus
8. The Cultural Apparatus⁴

To appreciate the ambitious conceptual scope of his model, consider how Althusser describes a shift in the dominance of one Apparatus over the others: whereas the “Religious Apparatus” prevailed for many centuries in Europe, Althusser contends, “The fact is that *the Church has today been replaced by the school*: it has succeeded it and occupies its *dominant* sector [...]”⁵ It is in this sector, the philosopher explains, where “the relations of the exploited to the exploiters and exploiters to exploited” are fortified and reproduced — in a “process of acquiring what comes down, in the end, to a handful of limited types of know-how [...]”⁶

Volumes could be written on how Althusser's depiction of the role of the "Scholastic Apparatus" in reproducing capitalist ideologies plays out in Annandale-on-Hudson, but for my purposes in this project I narrow in on one particular question left open in his work, that is, on the dominance of one "mode of production" over others. Defining Ideological State Apparatuses in terms of how the *productive forces* (human labor and physical material) both reinforce and are reinforced by the *relations of production* (social relations between "agents of production" and those "*who are not agents of production*"⁷), early in his work Althusser alludes to some kind of enigmatic "*unity*" between these two sides, carrying true across all the different *modes of production* in a given society. He insists that in a "concrete social formation," this unity is "conferred" upon all other modes of production by one dominant mode of production.⁸ To what can we attribute this intricate harmony? "The principal difficulty [...] has to do with the plural of the 'productive forces' belonging to *one* given mode of production." While Althusser succeeded in articulating ISAs in terms of a singular dominant system — the "scholastic system" — he struggled to formulate the same 'unifying' operation for the various *modes of production*. He wrote, "This in itself is a problem for which we do not yet have a real theory."⁹

To answer to this problem, I propose we turn to the Internet: digital digital technology companies today symbolize the dominant mode of production in our society. They determine the dominant relations of production by way of two main interventions, the first of which could be the topic of another Senior Project: their material dominance over traditional industries, and a linguistic dominance over public discourse. Rapid vertical integration in the online retail industry over the past two decades (Amazon for example) emulates the phenomenon by which, as Althusser described, "several modes of production 'coexist' under the dominance of one of

them.”¹⁰ Meanwhile, the proliferation of “managerial censorship” systems on digital media platforms — not to mention blatant censorship or disinformation campaigns — indicates the profound relationship between social networking and dominant ideologies. Kate Klonick’s theory of the “New Governors” supports this thesis, in that she clearly defines social media companies on the same level conceptually as governments and citizens with concern to establishing First Amendment norms and a collective definition for free speech. In fact, the subtler forms of influence described by Klonick, Jiang Ying and Robert Post closely resemble a distinct State Ideological Apparatus, as Althusser pointed out, “The Ideological State Apparatuses cannot be called repressive in the same sense as the ‘state apparatus’ because they do not, by definition, use physical violence. [...] they function, not ‘on violence’, but ‘on ideology’.”¹¹ Whereas “repression” remains a useful term for traditional free speech-based criticisms of Internet traffic manipulation, the medium’s most dire consequences may indeed stem from examples outside the category of repression. For these reasons, reconceptualizing Internet governance in terms of the dominant mode of production globally, and framing social media companies as a dominant Ideological State Apparatus, will prove key in future efforts both to develop more cohesive regulatory systems and to settle on adequate new theoretical terminology for discussing the implication of the proliferation of social networks.

During Mark Zuckerberg’s testimony before Congress, Utah Senator Orrin Hatch exhibited a profound (but not rare) lack of understanding about how Facebook operates, asking, “How do you sustain a business model in which users don’t pay for your service?”¹² At surface, Hatch embodied widespread confusion and ignorance about the most basic functions underlying

the social media industry. But by asking such a broad question, the Senator also demonstrated the extent to which legislators and users alike take for granted the immense powers social media companies have accrued over the past twenty years.¹³

Zuckerberg blinked slowly, then said with a smile, “Senator, we run ads.”¹⁴ In fact, Facebook generates more than \$30 billion a year in advertising revenue, making it the second-largest advertising network in the world after Google. Senator Hatch replied: “I see. That’s great.”¹⁵ — clearly unaware that the multi-year Russian influence campaign on the 2016 presidential election employed up to \$1.15 million worth of social media advertising *per month*, according to details unveiled by Special Counsel Robert Mueller six weeks before Zuckerberg’s hearing.¹⁶ While others proved more knowledgeable than Senator Hatch on the subject of the hearing — including Vermont Senator Patrick Leahy, who called Facebook “an unwitting co-conspirator in Russian interference,” and California Senator Kamala Harris, who prompted Zuckerberg to admit that leaders within the company decided not to inform users when they first learned of the breach in 2015 — the testimony at large encapsulated a broad trend of general ignorance among politicians and consumers alike regarding the extensive power Facebook wields over user data and privacy.

New York attorney, professor and former political candidate Zephyr Teachout went as far as to call the hearing “an utter sham” in an op-ed in *The Guardian*, citing Zuckerberg’s scripted responses and the five-minute limit on each period of questioning as signs that the entire hearing was more of a publicity stunt than a serious session. Teachout highlighted how the senators implicitly ceded authority to Zuckerberg through their ignorance, writing:

The worst moments of the hearing for us, as citizens, were when senators asked if Zuckerberg would support legislation that would regulate Facebook. I don't care whether Zuckerberg supports Honest Ads or privacy laws or GDPR. By asking him if he would support legislation, the senators elevated him to a kind of co-equal philosopher king whose view on Facebook regulation carried special weight. It shouldn't.¹⁷

By our own lack of understanding of the inner mechanisms and policies driving the platforms upon which we rely daily, we too, as users, grant tremendous power to the “philosopher-king” archetype of the CEOs and VCs of Silicon Valley. (Although, in ‘our’ defense, *The Atlantic* published a study in 2012 suggesting that for an average American to read every privacy policy they encounter in a single year would take 76 work days.¹⁸) Something similar could be said for the Bard student who knows nothing of the corruption festering in Sottery Hall. Teachout's sharp reading of the Zuckerberg hearing also resonates with Althusser's description of the scholastic Ideological State Apparatus: what he referred to as “an ideology which depicts the school as a neutral environment free of ideology (because it is... not religious) where teachers are respectful of the ‘conscience’ and ‘freedom’ of the children entrusted to them.”¹⁹ Sound familiar? Similarly, in our individual perceptions of different social media companies, or of different corners of the Internet, digital platform websites condition us to believe we are operating through a medium free of ideology.

The implications of our collective submission to techno-authority are far-reaching, and probably more significant than can be comprehended in the present moment. Beyond the hot-button political affairs and crises of the today's front page news, scholars point out that there

exist deeper and longer-term threats to the integrity of interpersonal relationships between individuals borne in the ubiquity of the Internet, social networking platforms and other digital technology industries. We as individuals are caught in the crossfire of a corporate oligopoly fighting not just for our money, but for our attention, for the finite number of minutes we have in a day to consume not just through our wallets, but through our ears, eyes and fingers. How do these forces sway the individual's emerging sense of self? Wendy Hui Kyong Chun's recent work on network theory proves pertinent to this line of questioning. She wrote: "[Networks] figure connections and flow—and constantly produce crises—by linking and breaching the personal and the collective, the political and the technological, the biological and the machinic [sic], the theoretical and the empirical."²⁰ By both "linking and breaching" fundamental paradigms in theories on self and society, the Information Age thus challenges members of the network society to grasp the incomprehensible, or worse, fools us into believing that Excel can help with this process.

Harvard psychologists Howard Gardner and Kate Davis examined the real-world manifestations of what Chun called our new, network-based "neoliberal collectivity" in *The App Generation*, remarking in their introduction on the qualities distinguishing the Internet from previous information and communications technologies:

In sharp distinction to the mass media of the last century, they are intensively personal and invite activity on the part of the user: *personal* in the sense that the individual user is (in contrast to radio or television) increasingly in control of what is received and when it is received; inviting *activity* in the sense that (again, in contrast to radio in television) it is easy and straightforward to transmit content

as well as to receive it and (in contrast to the telephone or the radio) in that digital devices can readily and actively involve the visual and tactile senses, as well as the auditory.²¹

In the eyes of members of my generation and those younger than myself, interaction through social media indeed often represents one of the most “personal” forms of expression and activity in a person’s day or even life. Simply consider the popularity of monetized YouTube channels based around nothing more than the premise of an individual’s personhood and their willful ‘materialization’ of that individuality through digital media.

Emulating the process through which prominent social media companies have crafted a unique niche in human rights scholarship for their relative freedom from real moral liability (through public relations synchronization with international rights and political leaders) young people as a result of their intensely personal relationships to social media “take care to present a socially desirable, *polished self* online,” as Gardner and Davis observed in their research. Crafting “strategic self-presentations by deciding what information to highlight, downplay, exaggerate or leave out entirely,” as they eloquently describe, in many ways characterizes modern psychologies of the self not just online, but offline too. The contemporary Italian philosopher Luciano Floridi urges us to extrapolate these psychologies of technology to material reality, or perhaps more accurately, identifies the inevitability of the phenomenon, writing: “we no longer live online or offline but *onlife*, that is, we increasingly live in that special space, or *infosphere*, that is seamlessly analogue and digital, offline and online.”²²

The notion of the ‘polished self’ can be helpful for explaining the consequences of what Mark Lilla called a “fixation on diversity” in liberal circles in America today in his 2016 article,

“The End of Identity Liberalism.”²³ Lilla explains that this “fixation on diversity,” a morally righteous vocabulary, “has produced a generation of liberals and progressives narcissistically unaware of conditions outside their self-defined groups, and indifferent to the task of reaching out to Americans in every walk of life.”²⁴ Based on how Davis and Gardner define the Internet in contrast to older technologies, maybe cultivating a narcissistic unawareness of the “conditions outside their self-defined groups” is exactly what social media, and the attachments we form to our constructed digital identities, were designed for.

Zooming out from the discussion of the ‘polished self’ on the level of the individual, we can also apply the similar concept to better understanding how Louis Althusser conceptualizes the power of the Ideological State Apparatus in shaping public discourse. In this chapter, I quite unscientifically suggested that social media symbolizes a dominant ISA, while the Internet symbolizes a dominant mode of production. To blur the lines between these assertions slightly, I conclude my project with this citation, a description by Althusser of the particular characteristics setting the dominant “Scholastic Apparatus” apart from other ISAs. He explained:

From nursery school on, the school takes children from all social classes and, from nursery school on and for years thereafter, the years when children are most ‘vulnerable’, stuck fast as they are between the scholastic and familial Ideological Apparatuses, pumps them full, with old methods and new, of certain kinds of ‘know-how’ (French, arithmetic, natural history, science, literature) packaged in the dominant ideology, or simply, of the dominant ideology in the pure state (ethics, civics, philosophy). [...] No other Ideological State Apparatus... has a captive audience of all the children of the capitalist social formation at its beck

and call (and — this is the least it can do — at not cost to them) for as many years as the schools do, eight hours a day, six days our of seven.²⁵

Whereas according to Althusser the the scholastic system took centuries to gradually replace the Church as a dominant ISA, another similar transition appears to have occurred in just the past two decades. Few in the 1970s, or even in the 1990s, could have predicted the extent to which the attention of the children “of the capitalist formation[s]” of the world (living comfortably in developed countries) would one day become inundated by digital networking platforms and other novel technologies to new extents. As Howard Gardner and Kate Davis illustrated in their research, this new reality is upon is.

In this project I have attempted to illustrate how classical theories and traditional paradigms fail to address the most pressing issues facing novel human rights, free speech and other activist work in the 21st century. We must strive to understand the forces at play in the mechanisms of Internet governance — or first, at least, embrace our uncertainty about the medium and reject presuppositions of ideological neutrality — for the future survival of our species may well depend on the capacity of individuals to maintain freedom of thought, expression and action in the face of a vast network of algorithms and machines designed to exploit the human body in new ways and in the interests of the powerful. Traditional free speech and human rights theories are waning, for the foundational precepts of liberal — from a metaphysical sovereignty of the individual to the infallibility of science and technology, the incontrovertible power of the state and the biblical reverence with which we devour *The New York Times* — are rendered irrelevant by an ongoing revolutions in the field of information and communications technologies (ICTs). If progressives wish to make a positive impact on the

future in the long-term, they must shift their focus from national governments and domestic issues to increasingly global, private networks of digital media and the administration of ICT infrastructures. While nation-states remain the foremost brokers of real repressive power in many cases today, this facet of society cannot be properly understood without first analyzing the private digital mechanisms subliminally influencing what and how people think. (For further reading, see “Babies And iPads Might Not Be Such A Great Combination After All,” by Carolyn Gregoire.²⁶)

Chapter 4 Notes

1. Statista. "U.S. Population With A Social Media Profile 2018" 2018.
<https://www.statista.com/statistics/273476/percentage-of-us-population-with-a-social-network-profile/> (accessed December 10, 2018).
2. McKenzie, Sheena. "Facebook's Mark Zuckerberg says sorry in full-page newspaper ads." CNN, March 25, 2018.
3. Senate Committee on the Judiciary, Senate Committee on Commerce, Science, and Transportation. "Facebook, Social Media Privacy, and the Use and Abuse of Data: Full Joint Committee Meeting." April 10, 2018.
<https://www.judiciary.senate.gov/meetings/facebook-social-media-privacy-and-the-use-and-abuse-of-data> (accessed December 10, 2018).
4. Althusser, Louis. *On the Reproduction of Capitalism: Ideology and Ideological State Apparatuses*. London: Verso, 2014: 75
5. Ibid., 147
6. Ibid., 146
7. Ibid., 27
8. Ibid., 20
9. Ibid., 26
10. Ibid., 25-26
11. Ibid., 78
12. House Committee on Science, Space and Technology. "Management of NSFNET. Hearing before the Subcommittee on Science of the Committee on Science, Space, and Technology, U.S. House of Representatives, One Hundred Second Congress, Second Session."
13. Kollewe, Julia. "Google And Facebook Bring In One-Fifth Of Global Ad Revenue." *The Guardian*, May 2, 2017.
<https://www.theguardian.com/media/2017/may/02/google-and-facebook-bring-in-one-fifth-of-global-ad-revenue> (accessed December 10, 2018). Statista. "U.S. Facebook Advertising Revenue 2018." 2018.
<https://www.statista.com/statistics/544001/facebooks-advertising-revenue-worldwide-usa/> (accessed December 10 2018).
14. Youtube Video. "Mark Zuckerberg testifies on Capitol Hill (full Senate hearing)." The Washington Post, April 10, 2018. <https://www.youtube.com/watch?v=6ValJMOpt7s>
15. House Committee on Science, Space and Technology. "Management of NSFNET. Hearing before the Subcommittee on Science of the Committee on Science, Space, and Technology, U.S. House of Representatives, One Hundred Second Congress, Second Session."
16. Nguyen, Tam. "Russian Spent \$1.25M Per Month on Ads, Acted Like an Ad Agency: Mueller." AdAge, February 16, 2018.
<https://adage.com/article/digital/russia-spent-1-25m-ads-acted-agency-mueller/312424/> (accessed December 10, 2018).
17. Teachout, Zephyr. "Mark Zuckerberg's Facebook Hearing Was An Utter Sham." *The Guardian*, April 11, 2018.
<https://www.theguardian.com/commentisfree/2018/apr/11/mark-zuckerbergs-facebook-hearing-sham> (accessed December 10, 2018).

18. Madrigal, Alexis C. "Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days." *The Atlantic*, March 1, 2012
19. 146 Althusser, *On the Reproduction of Capitalism: Ideology and Ideological State Apparatuses*.
20. Chun, Wendy Hui Kyong. Eds. Anna Watkins Fisher and Thomas Keenan. *New Media, Old Media: A History and Theory Reader*. New York: Routledge, 2016: 39
21. Gardner, Howard, and Katie Davis. *The App Generation: How Today's Youth Navigate Identity, Intimacy, and Imagination in a Digital World: With a New Preface*. New Haven: Yale University Press, 2014: 23
22. Floridi, Luciano. "Soft Ethics and the Governance of the Digital." *Philosophy & Technology* 31, no. 1 (March 2018): 1–8. <https://doi.org/10.1007/s13347-018-0303-9>
23. Lilla, Mark. "Opinion: The End Of Identity Liberalism". *The New York Times*, November 18, 2016.. Accessed December 10 2018. <https://www.nytimes.com/2016/11/20/opinion/sunday/the-end-of-identity-liberalism.html> (accessed December 10, 2018).
24. Ibid.
25. 145–146 Althusser, *On the Reproduction of Capitalism*.
26. Gregoire, Carolyn. "Babies And iPads Might Not Be Such A Great Combination After All." *The Huffington Post*, September 23, 2018. https://www.huffingtonpost.com/entry/babies-ipad-screens_us_56019e09e4b00310edf8ce12 (accessed December 10, 2018).

Bibliography

(For court cases, newspapers and other non-scholarly works, see chapter endnotes.)

Abbate, Janet. "Government, Business, and the Making of the Internet." *The Business History Review* 75, no. 1 (2001): 147-76. <http://www.jstor.org/stable/3116559> (accessed December 10, 2018).

ACLU to Senate Commerce committee, November 7, 2017.

<https://www.aclu.org/letter/aclu-letter-opposing-sesta> (accessed December 10, 2018).

Adeyah, Catherine N. "Information and Communication Technologies in Africa: A Review and Selective Annotated Bibliography: 1990-2000." International Network for the Availability of Scientific Publications, 2001. 38–38.

<https://pdfs.semanticscholar.org/64f6/7e24663009d85e96a888979950a60c779e49.pdf> (accessed November 16, 2018).

Althusser, Louis. *On the Reproduction of Capitalism: Ideology and Ideological State Apparatuses*. London: Verso, 2014: 75.

Andjelkovic, Maja, Don MacLean, and Tony Vetter. *Internet Governance and Sustainable Development: Towards a Common Agenda*. Winnipeg: International Institute for Sustainable Development, October 2007.

https://www.iisd.org/pdf/2007/igsd_common_agenda.pdf (accessed November 12, 2018).

Antonio, Robert J., and Alessandro Bonanno. "A New Global Capitalism? From 'Americanism and Fordism' to 'Americanization-Globalization.'" *American Studies* 41, no. 2/3 (2000): 33-77. <http://www.jstor.org/stable/40643230> (accessed November 17, 2018).

Aoki, Keith. "Considering Multiple and Overlapping Sovereignties: Liberalism, Libertarianism, National Sovereignty, 'Global' Intellectual Property, and the Internet." *Indiana Journal of Global Legal Studies* 5, no. 2 (1998): 443-73. <http://www.jstor.org/stable/25691115> (accessed November 10, 2018).

Apodaca, Clair. "Global Economic Patterns and Personal Integrity Rights after the Cold War." *International Studies Quarterly* 45, no. 4 (2001): 587-602.

<http://www.jstor.org/stable/3096061> (accessed November 12, 2018).

- Arendt, Hannah. "The Public and the Private Realm." In *The Human Condition*. Chicago: University of Chicago Press, 1958.
- Armbrust, Walter. "The Revolution Against Neoliberalism." In *The Dawn of the Arab Uprisings: End of an Old Order?*. ed. Haddad Bassam, Bsheer Rosie, and Abu-Rish Ziad, by Owen Roger. London: Pluto Press, 2012: 122. doi:10.2307/j.ctt183p77h.23.
- Ball, Patrick, Mark Girouard, and Audrey Chapman. "Information Technology, Information Management, and Human Rights: A Response to Metzl." *Human Rights Quarterly* 19, no. 4 (1997): 836-59. <http://www.jstor.org/stable/762688>.
- Bennett, Colin J. "Computers, Personal Data, and Theories of Technology: Comparative Approaches to Privacy Protection in the 1990s." *Science, Technology, & Human Values* 16, no. 1 (1991): 51-69. <http://www.jstor.org/stable/690039> (accessed November 10, 2018).
- Blanton, Shannon Lindsey. "Foreign Policy in Transition? Human Rights, Democracy, and U.S. Arms Exports." *International Studies Quarterly* 49, no. 4 (2005): 647-67. <http://www.jstor.org/stable/3693504> (accessed November 12, 2018).
- Bomse, Amy Lynne. "The Dependence of Cyberspace." *Duke Law Journal* 50, no. 6 (2001): 1717-749. doi:10.2307/1373046.
- Boutros-Ghali, "Empowering the United Nations." (1992).
- Brenkert, George G. "Google, Human Rights, and Moral Compromise." *Journal of Business Ethics* 85, no. 4 (2009): 453-78. <http://www.jstor.org/stable/40294808>.
- Camp, Jean and Y.T. Chien. "The Internet as Public Space: Concepts, Issues, and Implications in Public Policy." *ACM SIGCAS Computers and Society* 30, no. 13 (September 2000). https://sites.hks.harvard.edu/m-rcbg/research/j.camp_acm.computer_internet.as.public.space.pdf (accessed December 7, 2018).
- Campbell, Sharon. "Youthreach: Guidelines for Writing Children's Internet Policies." *American Libraries* 29, no. 1 (1998): 91-92. <http://www.jstor.org/stable/25634797> (accessed November 18, 2018).
- Campbell, Tom. "A Human Rights Approach to Developing Voluntary Codes of Conduct for Multinational Corporations." *Business Ethics Quarterly* 16, no. 2 (2006): 255-69. <http://www.jstor.org/stable/3857824.1> (accessed November 5, 2018).

- Carlsson, Ulla. "The Rise and Fall of NWICO." *Nordicom Review* 24 (2003).
https://www.researchgate.net/publication/314192925_The_Rise_and_Fall_of_NWICO
 (accessed November 10, 2018).
- Castells, Manuel. *The Information Age: Economy, Society, and Culture*. Chichester, West Sussex: Wiley-Blackwell, 2010. <https://books.google.com/books?id=hngg4aFtJVcC>.
- Chang, Jennifer C. "In Search of Fair Housing in Cyberspace: The Implications of the Communications Decency Act for Fair Housing on the Internet." *Stanford Law Review* 55, no. 3 (2002): 969-1012. doi:10.2307/1229678.
- Chun, Wendy Hui Kyong. Eds. Anna Watkins Fisher and Thomas Keenan. *New Media, Old Media: A History and Theory Reader*. New York: Routledge, 2016.
- Coates, Vary T. "The Future of Information Technology." *The Annals of the American Academy of Political and Social Science* 522 (1992): 45-56. <http://www.jstor.org/stable/1047418>
 (accessed November 10, 2018).
- Corrales, Javier and Frank Westhoff. "Information Technology Adoption and Political Regimes." *International Studies Quarterly* 50, no. 4 (2006): 911-33.
<http://www.jstor.org/stable/4092785> (accessed November 9, 2018).
- Clapham, Andrew. *Human Rights In The Private Sphere*. Oxford: Clarendon Press, 1993.
- Cullen, Robert. "Human Rights Quandary." *Foreign Affairs*, vol. 71, no. 5, 1992, pp. 87-88.
 JSTOR, JSTOR, www.jstor.org/stable/20045404 (accessed November 9, 2018).
- Denardis, Laura. "The Internet Governance Oxymoron." In *The Global War for Internet Governance*, 1-32. Yale University Press, 2014. <http://www.jstor.org/stable/j.ctt5vkz4n.3>
 (accessed November 9, 2018).
- "Developments in the Law: The Law of Cyberspace." *Harvard Law Review* 112, no. 7 (1999): 1597-1609. doi:10.2307/1342414.
- D'Haenens, Leen. "Beyond Infrastructure. Europe, The United States and Canada on the Information Highway: Where Business and Culture Collide." In *Images of Canadianness: Visions on Canada's Politics, Culture, and Economics*, ed. D'Haenens Leen, 237-54. Ottawa: University of Ottawa Press, 1998. <http://www.jstor.org/stable/j.ctt1cn6s1m.15>
 (accessed November 19, 2018).

- Dillon, John. The Internet Is Changing from a Public Resource to a Lucrative Operation Influenced by Spooks and Former Pentagon Officials. Open Access and Information are Increasingly Controlled.” *CovertAction Quarterly*.
[youhttps://web.archive.org/web/20101128041749/http://mediafilter.org/caq/internic](https://web.archive.org/web/20101128041749/http://mediafilter.org/caq/internic)
 (accessed December 10, 2018).
- Donnelly, Jack. "Human Rights and Foreign Policy." In *Universal Human Rights in Theory and Practice*, 197-214. Ithaca; London: Cornell University Press, 2013.
<http://www.jstor.org/stable/10.7591/j.ctt1xx5q2.16> (accessed November 14, 2018).
- . "Human Rights in the New World Order." *World Policy Journal* 9, no. 2 (1992): 249-77. <http://www.jstor.org/stable/40209249> (accessed November 9, 2018).
- Erdos, David. "Fundamentally Off Balance: European Union Data Protection Law And Media Expression." *University of Cambridge Faculty of Law Research Paper* no. 42 (July 25, 2014). SSRN Electronic Journal. doi:10.2139/ssrn.2471531.
- Falk, Richard. "Interpreting the Interaction of Global Markets and Human Rights." In *Globalization and Human Rights*, edited by Brysk Alison, 61-76. Berkeley; Los Angeles; London: University of California Press, 2002.
<http://www.jstor.org/stable/10.1525/j.ctt1pnh0f.8> (accessed November 9, 2018).
- Fanon, Frantz. *A Dying Colonialism*. New York: Grove, 1967: 75.
- Faucette, Jeffrey E. "The Freedom of Speech at Risk in Cyberspace: Obscenity Doctrine and a Frightened University's Censorship of Sex on the Internet." *Duke Law Journal* 44, no. 6 (1995): 1155-182. doi:10.2307/1372937.
- Feingold, Russ. In 141 Cong. Rec. S8335 (June 14, 1995).
<https://www.congress.gov/congressional-record/1995/06/14/senate-section/article/S8310-3>
 (accessed November 20, 2018).
- Fiss, Owen. "The Censorship of Television." In Bollinger, Lee C., and Geoffrey R. Stone. *Eternally Vigilant: Free Speech in the Modern Era*. Chicago: University of Chicago Press, 2002.
- Floridi, Luciano. "Soft Ethics and the Governance of the Digital." *Philosophy & Technology* 31, no. 1 (March 2018): 1–8. <https://doi.org/10.1007/s13347-018-0303-9>

- (2012). *The Fourth Revolution. The Philosophers' Magazine* 57: 96-101.
<https://philpapers.org/rec/FLOTFR>.
- Forsythe, David P. "Human Rights Fifty Years after the Universal Declaration." *Political Science and Politics* 31, no. 3 (1998): 505-11. doi:10.2307/420608.
- Freedomhouse.org. "Venezuela Country Profile." Freedom on the Net 2017.
<https://freedomhouse.org/report/freedom-net/2017/venezuela> (accessed December 10, 2018).
- Gardner, Howard, and Katie Davis. *The App Generation: How Today's Youth Navigate Identity, Intimacy, and Imagination in a Digital World: With a New Preface*. New Haven: Yale University Press, 2014: 23.
- General Data Protection Regulation*. European Union (2016/679). <https://gdpr-info.eu/> (accessed December 7, 2018).
- Ghonim, Wael. Quoted in Doran, Michael S. et al. "The Impact of New Media: The Revolution Will Be Tweeted." In *The Arab Awakening: America and the Transformation of the Middle East*, 39-46. Brookings Institution Press, 2011.
<http://www.jstor.org/stable/10.7864/j.ctt1280ww.9> (accessed December 7, 2018).
- Goldsmith, Jack L. "Against Cyberanarchy." *Occasional Papers from the Law School: University of Chicago* (1999): 40.
http://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1001&context=occasional_papers (accessed November 19, 2018).
- Goodman, S, Press, L, Ruth, S., and Rutkowski, A., "The Global Diffusion of the Internet: Patterns and Problems," *Communications of the ACM* 37, No 8, (August 1994): 27-31.
<http://som.csudh.edu/cis/lpress/sy.htm> (accessed November 8, 2018).
- Harvard Law Review. "Note: 'Section 230 As First Amendment Rule.'" <https://harvardlawreview.org/2018/05/section-230-as-first-amendment-rule/> (accessed November 29 2018).
- Hellweg, Eric. "The First Big Data Election." *Harvard Business Review*, November 13, 2012

- <https://hbr.org/2012/11/2012-the-first-big-data-electi> (accessed December 10, 2018).
- House Committee on Science, Space and Technology. "Management of NSFNET. Hearing before the Subcommittee on Science of the Committee on Science, Space, and Technology, U.S. House of Representatives, One Hundred Second Congress, Second Session." <https://eric.ed.gov/?id=ED350986>.
- Houser, Kimberly A. and W. Gregory Voss. "GDPR: The End of Google and Facebook or a New Paradigm in Data Privacy?" *Journal of Law & Tech.* no. 1 (2018).
- Human Rights Watch. "Venezuela: Events of 2017." 2018. <https://www.hrw.org/world-report/2018/country-chapters/venezuela#> (accessed December 10, 2018).
- Human Rights Watch. "Venezuela: TV Shutdown Harms Free Expression." May 21, 2007. <https://www.hrw.org/news/2007/05/21/venezuela-tv-shutdown-harms-free-expression> (accessed December 10, 2018).
- Hussain, Farooq. "Historic Role Of The Commercial Internet eXchange Router And Its Impact On The Development Of Internet eXchange Points [IXs]." Historical Role of the CIX Router. October 2, 2003. <https://web.archive.org/web/20070316024259/http://www.farooqhussain.org/projects/Historic%20Role%20of%20the%20CIX%20Router%2010-03-03.pdf> (accessed December 10, 2018).
- International Council on Human Rights Policy. "Journalism, Media and the Challenge of Human Rights Reporting," ICHRP. Geneva, Switzerland, 2002. 77. <https://ssrn.com/abstract=1551233> (accessed November 9, 2018).
- Interviewee Schrage, Elliot. "New Media Tools and Public Diplomacy." Interview by Lee Hudson Teslik. *Council on Foreign Relations*, May 4, 2009 <https://www.cfr.org/interview/new-media-tools-and-public-diplomacy> (accessed December 10, 2018).
- Jabine, Thomas B., and Richard P. Claude, eds. "Human Rights and Statistics: Getting the Record Straight." Philadelphia: University of Pennsylvania Press, 1992. <http://www.jstor.org/stable/j.ctv512twg> (accessed November 10, 2018).

- Jasanoff, Sheila, and Dorothy Nelkin. "Science, Technology, and the Limits of Judicial Competence." *Science* 214, no. 4526 (1981): 1211-215. <http://www.jstor.org/stable/1687754> (accessed November 8, 2018).
- Ying, Jiang. "Chinese Anger at the Label of Censorship." In *Cyber-Nationalism in China: Challenging Western Media Portrayals of Internet Censorship in China*, 63-76. South Australia: University of Adelaide Press, 2012. <http://www.jstor.org/stable/10.20851/j.ctt1sq5x62.9>.
- Josselin, D. & W. Wallace "Non-State Actors in World Politics: A Framework." In *Non-state Actors in World Politics*, ed. Josselin, D & W. Wallace. Basingstoke: Palgrave (2001).
- Kangulu, C.M., and F.E. Wood. "An Evaluation of the Pan-African Development Information System (PADIS): With Particular Reference to Zambia." *Journal of Information Science* 21, no. 5 (October 1995): 343-57. doi:10.1177/016555159502100502.
- Keck, Margaret E., and Kathryn Sikkink. "Human Rights Advocacy Networks in Latin America." In *Activists beyond Borders: Advocacy Networks in International Politics*, 79-120. Cornell University Press, 1998. <http://www.jstor.org/stable/10.7591/j.ctt5hh13f.6> (accessed November 10, 2018).
- Keller, Daphne. "Free Expression Gaps In The General Data Protection Regulation." The Center for Internet and Society, November 30, 2015. <http://cyberlaw.stanford.edu/blog/2015/11/free-expression-gaps-general-data-protection-regulation> (accessed December 8 2018).
- Klonick, Kate. "The New Governors: The People, Rules, and Processes Governing Online Speech" *Harvard Law Review* 131, no. 6 (April 2018) https://harvardlawreview.org/wp-content/uploads/2018/04/1598-1670_Online.pdf (accessed November 9, 2018).
- Laudon, Kenneth C. "Markets And Privacy". *Communications Of The ACM* 39, no. 9 (1996): 92-104. aisel.aisnet.org/cgi/viewcontent.cgi?article=1025&context=icis1993 (accessed November 10, 2018).

- Langlois, Anthony J. "Human Rights: The Globalisation and Fragmentation of Moral Discourse." *Review of International Studies* 28, no. 3 (2002): 484.
<http://www.jstor.org/stable/20097807> (accessed November 9, 2018).
- Luke, Timothy W. "Cyberspace as Meta-Nation: The Net Effects of Online E-Publicanism." *Alternatives: Global, Local, Political* 26, no. 2 (2001): 136.
<http://www.jstor.org/stable/40645013> (accessed November 18, 2018).
- MacKinnon, Rebecca. "Race to the Bottom: Corporate Complicity in Chinese Internet Censorship." *Human Rights Watch* 18, No. 8(C) (August 2006) August 9, 2006
<https://www.hrw.org/sites/default/files/reports/china0806webwcover.pdf> (accessed November 8, 2018).
- Machill, Dr. Marcel, Machill Jens Waltermann. "Self-regulation as a Foundation." In *Self-regulation of Internet Content*, Gütersloh: Bertelsmann Foundation (1999), 21–28.
<https://www.cdt.org/files/speech/BertelsmannProposal.pdf> (accessed November 22, 2018).
- Maloney, Marilyn C. "Intellectual Property in Cyberspace." *The Business Lawyer* 53, no. 1 (1997): 236. <http://www.jstor.org/stable/40687783>.
- Mêgnigbêto, Eustache, and Maxime Hounton. "Fortunes and Misfortunes of the CENADI in Bénin: How a National Documentation Center Disappeared." *Journal of Information Policy* 3 (2013): 59-76. doi:10.5325/jinfopoli.3.2013.0059.
- Metzl, Jamie F. "Information Technology and Human Rights." *Human Rights Quarterly* 18, no. 4 (1996): 705-46. <http://www.jstor.org/stable/762590>.
- Mill, John Stuart. *On Liberty*. Kitchener, Ontario: Batoche Books Limited, 2001.
- Morris, John B. Jr. "The Past, Present, and Future of Internet Censorship and Free Speech Advocacy." In *Defending the First: Commentary on First Amendment Issues and Cases*. Ed. Joseph Rossumano. Mahwah: Lawrence Erlbaum Associates (2005). 189.
<https://books.google.com/books?id=FwKQAgAAQBAJ> (accessed November 17, 2018).
- Movius, L. "Global Debates on the Right to Communicate." *Global Media Journal* 7, no. 13, (2008).
<http://www.globalmediajournal.com/open-access/global-debates-on-the-right-to-communicate.pdf> (accessed November 9, 2010).

- Minović, Adriana. "GDPR: Integrating Human Rights into Business Practices." DipliFoundation, November 13, 2017.
<https://www.diplomacy.edu/blog/gdpr-integrating-human-rights-business-practices>
 (accessed December 7, 2018).
- Muchlinski, Peter T. "Human Rights and Multinationals: Is There a Problem?" *International Affairs* 77, no. 1 (2001): 31-47. <http://www.jstor.org/stable/2626552> (accessed November 9, 2018).
- Myers, Ken S., "Wikimmunity: Fitting the Communications Decency Act to Wikipedia." *Harvard Journal of Law and Technology*, Vol. 20, p. 163, Fall 2006; Berkman Center Research Publication No. 2006-08. SSRN: <https://ssrn.com/abstract=916529> (accessed November 24, 2018).
- Office of Inspector General, National Science Foundation. "Review of NSFNET." NSF, April 23, 1993. <https://www.nsf.gov/pubs/stis1993/oig9301/oig9301.txt> (accessed December 2018).
- Ornstein, Norman J., and Mark Schmitt. "Dateline Campaign '92: Post-Cold War Politics." *Foreign Policy*, no. 79 (1990): 169-86. doi:10.2307/1148683.
- Penney, Jonathon W. "Internet Access Rights: A Brief History and Intellectual Origins," *William Mitchell Law Review* 38, no. 1 (2011). <https://open.mitchellhamline.edu/wmlr/vol38/iss1/11> (accessed November 9, 2018).
- Post, Robert. C. "Data Privacy and Dignitary Privacy: Google Spain, the Right to Be Forgotten, and the Construction of the Public Sphere." Yale Law School, Public Law Research Paper No. 598 (April 2017). <https://ssrn.com/abstract=2953468> (accessed December 7, 2018).
- Post, Robert. C. "Democracy, Expertise and Academic Freedom: a First Amendment Jurisprudence for the Modern State," (2012). In 532 Vladeck, "Democratic Competence, Constitutional Disorder, and the Freedom of the Press."
- Sandler, Alyson. "Senators Klobuchar and Kennedy Introduce Privacy Legislation." *Inside Privacy*, April 25, 2018.
<https://www.insideprivacy.com/united-states/congress/senators-klobuchar-and-kennedy-introduce-privacy-legislation/> (accessed December 7, 2018).

- Schiller, Herbert I. "Is There a United States Information Policy?" In Preston, William, Edward S. Harman, Herbert I. Schiller, Sean Macbride, Ellen Ray, and William H. Schaap. *Hope and Folly: The United States and UNESCO, 1945-1985*. University of Minnesota Press, 1989. <http://www.jstor.org/stable/10.5749/j.cttttxk3> (accessed November 9, 2018).
- Senate Committee on the Judiciary, Senate Committee on Commerce, Science, and Transportation. "Facebook, Social Media Privacy, and the Use and Abuse of Data: Full Joint Committee Meeting." April 10, 2018. <https://www.judiciary.senate.gov/meetings/facebook-social-media-privacy-and-the-use-and-abuse-of-data> (accessed December 10, 2018).
- Shah, Rajiv C. and Jay P. Kesan. "The privatization of the Internet's Backbone Network." *Journal of Broadcasting and Electronic Media* 51, no. 1. (January 2001). 93-109. <https://doi.org/10.1080/08838150701308077>.
- Shahid Akhtar, ed. *National Information and Information Policies in Africa: Report and Proceedings of a Regional Seminar Held in Addis Ababa, Ethiopia*. International Development Research Centre & Pan African Documentation and Information System. November 28 – December 1, 1988. 117, 135–136. <https://www.ircwash.org/sites/default/files/501-90NA-7247.pdf> (accessed November 16, 2018).
- Simon, Glenn E. "Cyberporn and Censorship: Constitutional Barriers to Preventing Access to Internet Pornography by Minors." *The Journal of Criminal Law and Criminology* 88, no. 3 (1998): 1015-048. doi:10.2307/3491360.
- Slotnick, Allison. "'Friend' the President: Facebook and the 2008 Presidential Election." In *Politicking Online: The Transformation of Election Campaign Communications*, edited by Panagopoulos Costas, 249-71. New Brunswick, NJ; London: Rutgers University Press, 2009. <http://www.jstor.org/stable/j.ctt5hj455.18>.
- Smith, Aaron. "The Internet's Role In Campaign 2008." Pew Research Center (2009). <http://www.pewinternet.org/2009/04/15/the-internets-role-in-campaign-2008/> (accessed December 10, 2018).

- Smith, Linda et al. "Joint Statement in Response to Tech Industry Obstruction of Section 230 Legislation." August 2018.
<http://www.iamjanedofilm.com/wp-content/uploads/2017/08/Section-230-Statement-Myths-and-Facts...pdf> (accessed December 7, 2018).
- Sorensen, Karen. "Silencing the Net: The Threat to Freedom of Expression On-line," ed. Gara LaMarche. *Human Rights Watch* 8, no. 2 (May 1996)
<http://www.mtholyoke.edu/~cagora/technology/nyt/12-96.htm> (accessed November 16, 2018).
- Steele, Shari. "Taking a Byte Out of the First Amendment: How Free Is Speech in Cyberspace?" *Human Rights* 23, no. 2 (1996): 14-16. <http://www.jstor.org/stable/27879976> (accessed November 15, 2018).
- Sterling, Bruce. "Conferences on the Well" in *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*. Project Gutenberg (June 19, 2008).
<http://www.gutenberg.org/files/101/101-h/101-h.htm> (accessed November 13, 2018).
- Sunstein, Cass R. "The Future of Free Speech" in Bollinger, Lee C., and Geoffrey R. Stone. *Eternally Vigilant: Free Speech in the Modern Era*. Chicago: University of Chicago Press, 2002.
- "Supplement no. 7." In Economic and Social Council. "Economic Commission for Africa Annual Report: 29 March 1979-12 April 1980." *Economic and Social Council Official Records*. New York: United Nations (1980): 70.
https://digitallibrary.un.org/record/195718/files/E_1980_27%26E_CN-14_781_Rev-1-EN.pdf (accessed November 21, 2018).
- Talbot, David. 2012. "Facebook: The Real Presidential Swing State." *MIT Technology Review*, July 20, 2012.
- Taylor, Emily. "The Privatization of Human Rights: Illusions of Consent, Automation and Neutrality." In *Global Commission on Internet Governance*. Chatham House: Royal Institute of International Affairs (January 2016).
https://www.cigionline.org/sites/default/files/gcig_no24_web_2.pdf (accessed November 13, 2018).

- Thomas J. Johnson & David D. Perlmutter (2010) Introduction: The Facebook Election, *Mass Communication and Society*, 13:5, 554-559, DOI: 10.1080/15205436.2010.517490 (PDF) *Introduction: The Facebook Election*. Available from:
https://www.researchgate.net/publication/254306502_Introduction_The_Facebook_Election (accessed December 10, 2018).
- Tyson, Brady, and Abdul Aziz Said. "Human Rights: A Forgotten Victim of the Cold War." *Human Rights Quarterly* 15, no. 3 (1993): 589-604. doi:10.2307/762612.
- United Nations Department of Economic and Social Affairs. "Chapter XIX - Privacy: Changing Boundaries." In *2001 Report on the World Social Situation*. Inclusive Social Development, 2001.
<https://www.un.org/development/desa/dspd/report-on-the-world-social-situation-rwss-social-policy-and-development-division/2001-report-on-the-world-social-situation.html> (accessed November 16, 2018).
- Van Eecke, Patrick. "ECJ rules 'right to be forgotten' applies to search engines." International Association of Private Professors, May 13, 2014.
<https://iapp.org/news/a/ecj-rules-right-to-be-forgotten-applies-to-search-engines/> (accessed December 7, 2018).
- Van Ness, Peter, and Nikhil Aziz. *Debating Human Rights*. London: Routledge, 1999.
- Vise, David A. "Google." *Foreign Policy*, no. 154 (2006): 23.
<http://www.jstor.org/stable/25462030> (accessed November 9, 2018).
- Vladeck, Stephen I. "Democratic Competence, Constitutional Disorder, and the Freedom of the Press." *Washington Law Review* 87 (2012)
<http://digital.law.washington.edu/dspace-law/bitstream/handle/1773.1/1141/87WLR0529.pdf> (accessed December 7, 2018).
- Volokh, Eugene. "Cheap Speech and What It Will Do." *The Yale Law Journal* 104, no. 7 (1995): 1805-850. doi:10.2307/797032.
- Wallich, Paul. "Watch Your Electronic Mouth." *Scientific American* 271, no. 6 (1994): 43-44.
<http://www.jstor.org/stable/24942941> (accessed November 15, 2018).

- . "Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking about You." *Stanford Law Review* 52, no. 5 (2000): 1061. doi:10.2307/1229510.
- Wacks, Raymond. "Are Privacy and Free Speech Possible in Cyberspace?" In *Law, Morality and the Private Domain*, 269-90. Hong Kong University Press, 2000. <http://www.jstor.org/stable/j.ctt2jbz87.14> (accessed November 10, 2018).
- Williams, Christin B. and Girish J. Gulati. "The Political Impact of Facebook: Evidence from the 2006 Elections and the 2008 Nomination Contest." In *Politicking Online: The Transformation of Election Campaign Communications*, ed. Panagopoulos Costas, 272-91. New Brunswick, NJ; London: Rutgers University Press, 2009. <http://www.jstor.org/stable/j.ctt5hj455.19>.
- Wimmer, Kurt. "Free Expression And EU Privacy Regulation: Can The GDPR Reach U.S. Publishers?" *Syracuse Law Review* 68 (June 2018). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3188974. (accessed December 7, 2018).
- Wiseberg, Laurie S. "Access to United Nations Human Rights Documentation." *Human Rights Quarterly* 19, no. 2 (1997): 350-64. <http://www.jstor.org/stable/762580> (accessed November 20, 2018).
- World Conference on Human Rights. "Vienna Declaration and Programme of Action." Vienna: UN Human Rights Office of the high Commissioner (June 25, 1993). <https://www.ohchr.org/en/professionalinterest/pages/vienna.aspx> (accessed November 13, 2018).
- Wu, Timothy. "Application-Centered Internet Analysis." *Virginia Law Review* 85, no. 6 (1999): 1163-204. doi:10.2307/1073968.
- Yim, Joshua. "Section 230 and Fake News." *Northwestern University Law Review Online*, April 12, 2018. <http://blog.northwesternlaw.review/?p=868> (accessed December 7, 2018).

Yuval Noah Harari, *Homo Deus: A Brief History of Tomorrow*. Quoted in Zizek, Slavoj.

Incontinence of the Void: Economico-Philosophical Spandrels. Cambridge: The MIT Press
(2017): 132.