5-1-2015

Power Tangled in the Web: Assessing the Democratizing Power of Information and Communication Technologies

Patrick Kerr
College of the Holy Cross, pck15@protonmail.com

Power Tangled in the Web: Assessing the Democratizing Power of Information and Communication Technologies

By: Patrick Kerr

1 May 2015

Readers:
Professor Judith Chubb
Professor Daniel Klinghard
Professor Maria Rodrigues

Contents:

Introduction

> *There is no reason to believe that the foundation for liberty in cyberspace will simply emerge. Indeed, the passion for that anarchy—as in America by the late 1890s, and as in the former Eastern bloc by the late 1990s—has faded. Thus as, our framers learned, and as the Russians saw, we have every reason to believe that cyberspace, left to itself, will not fulfill the promise of freedom. Left to itself, cyber-space will become a perfect tool of control.* –Lawrence Lessig, *Code 2.0* (4).

Put simply, this is a thesis about technology. Yet often technology is conceptualized as simply machines; however, the idea of technology rooted in human practices is less appreciated or disregarded altogether. The above quotation asserts that technology is not purely neutral. Rather, political and social forces shape technology and how people and governments interact with it. In this specific example, Lessig fears the unprecedented possibilities of control via the manipulation of a powerful tool like the Internet when designed for more nefarious purposes. Yet common experiences with information and communication technologies (ICTs) nationally and globally exhort a more liberalizing experience that champions the unparalleled connectivity of the Internet. The answer to whether these ICTs like the Internet, social networking sites, and cell phones are forces of democratization largely depends on the political contexts in which they are employed.

A definition of technology is useful before passing judgment on today's most sophisticated technologies. Technology is both a physical apparatus like the brain, but also a medium, or a mind—a use to which a physical apparatus is put, according to Neil Postman. Postman's book *Technopoly: The Surrender of Culture to Technology* meditates on how technology—something as simple as placing a quantitative value to human thoughts, like grading a student's paper—does not add or subtract something, "it changes everything" (Postman, 18). Postman concludes that "technology always has unforeseen consequences, and it is not always clear, at the beginning, who or what will win, and who or what will lose" (Postman). For

example, Gutenberg, a stout Catholic, invented the printing press in hopes to unify the Holy Roman Empire, but in practice it was the seed of its destruction since it facilitated the fracture of the Church (Postman, 15). Similarly, monks invented the mechanical clock to organize prayer time, yet its contrivance enabled the tracking of "synchronization and controlling the actions of men," which in turn spurred capitalism (Postman, 14). Additionally, how a technology is used by a particular culture is not necessarily the only way it could be used (Postman lecture). Postman's work aims to salvage humanity from the overconsumption of technology and cautions against the readiness of society to adopt new technologies without considering how it impacts culture. Even though Postman was wary of this new technological society, his advice is clear: to not dissociate technology from human processes. Although written in 1992, Postman's ideas that caution against technology are extremely relevant in 2015 and drive the motivation for this thesis that seeks to assess whether ICTs impacts political power, and if so, at what costs?

Over the past year, there have been numerous examples of how technology has become more woven into daily political processes. In Hong Kong's Umbrella movement organizers, known as "keyboard fighters," used ICTs facilitated invaluable coordination and organization logistics (Beam, 1). These civil disobedient-styled protests garnered massive attention in their demands for "greater democracy," which even resulted in a live-television debate between political officials and young activists (Forsythe and Wong, 1). Additionally, ICTs like smart phone cameras captured several instances of police brutality that ignited protests in New York, New York and Baltimore, Maryland, leading to a public conversation about society that perhaps would not occur otherwise. This new digital age of connectivity was initially met with optimism that it would lead to more accountable leaders and transparent political processes. Some even

touted the Internet as being a tool for global democratization. Yet this is only one glimpse of a very complex picture of the ICT age.

This thesis questions the universality of ICTs as "liberation technology" and whether information and communication technologies (ICTs) enhance the political power of citizens in some capacities. To think more deeply about this question it helps to analyze how states react to such technology.

Increasingly, the world becomes more digitized. In the United States, recent figures show that smart phone ownership escalated from thirty-five percent in 2011 to sixty-four percent in 2014 (Pew Research). These statistics indicate a growing trend of how digital technologies play a larger role in our lives, and specifically, in our minute-to-minute actions. Like Postman says, "technologies create ways in which people perceive reality," which has shifted to an increased use and importance of ICTs (Postman, 21). Users receive their news and communicate with fellow citizens at the speed of their fingertips. No longer reliant on physical constraints of time and space, users enjoy immediate connectivity and convenience that the ICT age brings about. Yet this growing dependence on technology affects how users interact with politics and how they envision the future.

In the first chapter of the thesis, I survey the scholarly literature regarding whether ICTs are forces of democratization. Those who favor the liberalizing effects of the Web are labeled as cyber-utopians, whereas those who anticipate state control of the Internet as a means of reinforcing their power are known as "cyber-realists." This fissure begs the questions of whether ICTs facilitate political power in favor of the state or its citizens and whether future revolutions will be waged technologically. To test these competing hypotheses, I chose four case studies. My first case study, China—the epitome of Internet suppression—boasts the world's largest number

of Internet-connected users on the planet. However, the China Communist Party (CCP) does not show any signs of declining power due to the integration of ICTs. Rather, the case will be made that the Party's power has only grown stronger with the emergence of the Internet and the transformation of citizens into netizens.

My second case study assesses the role technology plays in the newly formed Islamic State of Syria and the Levant (ISIS). In the summer of 2014, ISIS captured global attention for their expansion from cities in Syria to northern areas of Iraq, including Mosul. For the purpose of this thesis, I analyzed their use of social media and gruesome viral videos that served various functions, including terror, prove of statehood, and terror all as a means of legitimizing their power. Unlike other fundamentalist groups, ISIS possesses territory and performs state-like duties and functions. Thanks to the Internet, I was able to analyze their videos as they were uploaded over the course of several months up until March 2015. Although ISIS may not yet possess state capabilities regarding the power of the Web, it demonstrates a keen ability to leverage power from ICTs that reinforces their power on the ground in the Levant.

My third case study of the 2011 Egyptian protests during the Arab Spring presents an example of how ICTs could act as "liberation technology" by generating grassroots mobilization that initiated a change in governance. Yet this is only partly true of what happened in Egypt from 2011 to 2013, when massive swaths of people called for President Mubarak's resignation, which he delivered in February 2011. Cell phones and Internet messaging networks facilitated mobilization by catalyzing existing alternative political networks. Since then, however, Egypt devolved into more chaos leading to the disempowerment of democratically-elected Mohammed Morsi in favor of "temporary" military order. Again, the analysis aims to assess the extent of the

role played by ICTs—if technology was liberating—in these uprisings, and also how the state and military benefit from controlling the networks in which the ICTs operate.

In my last case study, I analyze how both grassroots movements and the government use ICTs respectively. First, I focus on instances of digital mobilization in the United States with the 2011 Occupy movement and the impact of the cyber-vigilante group, Anonymous. Similar to the ICT-fueled organization noted in Tahrir Square, the Occupy movement spread across the U.S. in the Fall 2011 and across the globe. The second part of the chapter investigates the political efficacy of ICTs in the United States in the post-Edward Snowden era. The revelations made over the course of the Summer 2013 exposed the U.S.' intelligence agencies' remarkable capabilities in tracking, collecting, and storing data from all users' ICTs, unknown to technology companies and citizens.

As citizens' lives become more digital, political processes too become digital. Citizens gain more tools through which they can spread knowledge of their interests and political goals: social networking and sharing videos and photos allows for an unprecedented tool of connectivity. The power to connect is unquestioned; however, whether ICTs politically empower the masses remains ambiguous. Grassroots movements now require digital connectivity and thrive from making connections more easily and quickly. This power demonstrates itself in tangible ways in the physical turnout of people at political gatherings. Yet this presentation of grassroots power conflicts with the state's separate use of ICTs to control data and incubate political power.

Professor Daniel Klinghard describes technology as possessing a hidden form of control unbeknownst to the user. Likewise, this thesis aims to explore the disguised forms of control embedded in ICTs and how its uses vary in the four case studies. Although we remain in the

early years of the ICT era, the disguise of control embedded within ICTs is becoming clearer**.** Lessig's fears of ICTs as unprecedented tools of control have borne fruit and merit a closer, comparative analysis.

Chapter 1: Literature Review

The revolution of the Internet across the globe facilitates communication and makes information instantly available with network-connected devices. In line with a liberal democratic viewpoint, the Internet, or simply the Web, then must contain an inherent coding for democracy that utilizes this virtual connectedness to liberate oppressed populations. Instead of forcefully removing tyrants from power, the masses can tweet them out of their ostentatious palaces. This optimistic valuation of the Internet's sheer, potential force gives birth to a controversial idea, which Evgeny Morozov calls, *cyber-utopianism*: an ideology asserting that a new wave of democratization stems not from the breaking down of walls, but from wiring authoritarian nations with a ticking time bomb, the Internet.

The emergence of information and communication technologies (ICTs), like the Internet, e-mail, cell phones, and social networking sites, undoubtedly changes the way people interact on a micro-level, and accordingly, impacts how governments interact with their people and other states. The Internet does not destroy authoritarian regimes, instead the digital civil society created by ICTs facilitates the overthrow of tyrants in the twenty-first century. The development of more capable internet-connected devices and technologies presumes a new level of connectedness unprecedented in human history. Hence, the Web even earned itself a place on the U.S. State Department's list as a democratic right. Presidents, First Ladies, Secretaries of States, and foreign diplomats all endorsed the Internet in global speeches as a critical component of today's modern democracies. In 2010, Secretary of State Hilary Clinton proclaimed, "We stand for a single Internet where all of humanity has equal access to knowledge and ideas" (Diamond, 16). Still years later, in March 2014, First Lady Michelle Obama insinuated the importance of a virtual civil society in China, "It is so important for information and ideas to flow freely over the

Internet ... because that's how we discover the truth" (*Times*). It follows that by securing freedom of the Web, "freedom via the Web" can then occur in authoritarian regimes. The mantra from democratic nations like the United States champions the Internet as an inherently democratizing force. Such *cyber-utopianism* runs on "a naïve belief in the emancipatory nature of online communication" alongside a refusal to recognize that negative ICT impacts potentially burden society (Morozov, xiii).

It is true that the Web has been and can continue to be used to create more freedoms in several nations. The foundation of these arguments rests on a civil society created and fortified by the Internet. We can rely on classic democratic theories that are rejuvenated or recalculated to account for the variable of the Internet. From this civil society viewpoint, the Internet's democratizing force seeps into the most authoritarian regimes and breathes new political life into these "closed-off worlds." From the U.S' government point of view and many pro-Internet democratization scholars, ICTs produced a wave of optimism about the creation of freedoms in previously impenetrable authoritarian regimes.

Scholars like Larry Diamond see the Internet as a precondition for democracy, but also concede that the struggle for electronic access is "just the timeless struggle for freedom by new means. It is not technology, but people, organizations, and governments that will determine who prevails" (16). At this point, Diamond and others hope the Internet embodies democratic qualities in its ability to build an active civil society in once unreachable, authoritarian regimes. The traditional idea of civil society expands exponentially thanks to the Internet. The ability to communicate and organize without typical authoritarian repercussions allows a civil society to strengthen. Ideally, under this theory, a social movement demand more democratic rights until a society transitions to democracy.

Prior to the 2011 uprisings in North Africa and the Middle East, Philip N. Howard published, *The Digital Origins of Dictatorship and Democracy: Information Technology and Political Islam*, that in many ways prophesized the Arab Spring, or at the least the growing potential for uprisings in slowly democratizing Muslim nations. Howard emphasizes the capacity for political change embedded in the digital civil society. Building on earlier ideas of how empowering civil society can bring about democratic change, Howard sees the Web as a new avenue that can accelerate social and political change in authoritarian regimes once perceived as impenetrable. Howard asserts that ICTs are broken into four categories: wired political parties, a wired state, digital media, and a large online civil society, which facilitate the growth of these new counter-balances to traditional authoritarian control (199). Most importantly though, Howard finds that these ICTs erode authoritarian control and enlighten the populace since "information and communication technologies are the infrastructure for transposing democratic ideals from community to community" (199). In this vein, Howard lauds the Internet's ability to connect Muslim neighborhoods and states together and "provide new channels for mediating political discourse" (199). Thus, ICTs promote transparency and "improve the ability of civil society groups to monitor what their state is doing" (199).

Howard wholeheartedly believes that the Internet has reinforced civil society in the Middle East. First, Howard defines civil society groups as a "crucial part of all democracies" that is separate from the state (134). By developing space online for political debate uninhibited by authoritarian regimes, ICTs act "as the infrastructure for civil society" (135). His argument stresses how the Internet promotes "diverse new values, ideas and interests into social settings" (142). In addition civil society provides the necessary infrastructure and organization to run a social group, and serves a symbolic function of civil discourse absent in traditionally apolitical

societies (142). While acknowledging extremist elements on the Web, Howard insists that, "an active online civil society is a key ingredient of the causal recipe for democratization" (156). In contrast to Barrington Moore's classic work, *The Social Origins of Dictatorship and Democracy*, Howard argues that states in the Middle East are demonstrating the digital origins of contemporary dictatorships and democracies (200). Civil society combined with these "new information technologies" brings about democratic transition and "solidification" (201). While conceding that the state can use similar technologies to control information and manipulate the public, Howards believes the public's determination to circumvent controls ultimately triumphs:

> While there certainly are examples of how states use ICTs to control information and manipulate the public, there are far more examples of how ICTs are used by the public to get around the informational controls set up by states. Citizens…are no longer just consumers of political content, they manage the means of cultural production through consumer electronics. (201)

More importantly, Howard's argument stresses that political change is more evolutionary than revolutionary, and that the transition to democratization is "increasingly" a digital one (201).

Howard's 2013 book, *Democracy's Fourth Wave: Digital Media and the Arab Spring*, gives credence to his earlier ideas in which he declares that the uprisings demonstrate the effective of information technologies as, "a tool for gradually eroding centralized state power" (44). Again Howard's argument emphasizes the civil society on the Web as flourishing even at times of when the state cracks down (45). Howard pointedly illuminates his argument on page 34: "Social media have become the scaffolding upon which a functioning civil society can grow…[new] freedoms they did not have before: information networks not easily controlled by the state and coordination tools that are already embedded in trusted networks of family and friends." In his conclusion, Howard contends that countries that did not experience political uprisings lacked "a civil society equipped with digital scaffolding" (123). Hence, his argument spans both his books—civil society grew by producing its own content and remaining connected to

international news while also strengthening social networks that created a strong political solidarity. Lastly, Howard concedes that the political end results may be different and sporadic, but the uprisings themselves were digitally initiated by a vibrant digital civil society.

Larry Diamond's article "Liberation Technology" further develops this argument that ICTs counteract traditional authoritarian regimes. By using the Internet as an extension of the civil forum, ideas, commentaries and debates can enrich politically repressed populations in authoritarian regimes. Diamond lauds social networking sites as a key weapon against the government repression of information; he describes Twitter "as one of the most potent means for political and social networking and the rapid dissemination of news, views, and withering satire" (8). In unison Howard extols new media technologies, namely cell phones and the Internet, as "affect[ing] how individuals decide to participate or not participate in democratic actions" (199). Similarly, media pundits like Thomas Friedman celebrate how social media amplifies oppressed voices previously unheard in traditionally closed off regimes:

> The role of the Internet was overrated in Egypt and Tunisia. But it is underrated in the Gulf, where, in these more closed societies, Facebook, Twitter and YouTube are providing vast uncontrolled spaces for men and women to talk to each other — and back at their leaders. "I don't read any local newspapers anymore," a young Saudi techie told me. "I get all my news from Twitter. So much for government-controlled newspapers." (Freidman, Thomas. "The Other Arab Awakening," *New York Times*. 10/30/13)

Moreover, Diamond argues that there is simply too much information online on the various ICT mediums to possibly monitor and censor it all (8). The innovation of social media technologies directly changes the power relationship between the people and their state, thus encouraging cyber-utopians to see the Internet as a great weapon for building a digital civil society that can challenge authoritarian regimes.

Manuel Castells' *Networks of Outrage and Hope: Social Movements in the Internet Age* affirms the revolutionary power the Internet possesses for social movements. A veteran of the late 1960s protest movements, Castells personally describes his renewed optimism for social

protest facilitated by the decentralized power of the Web. Castells emphasizes how the Internet reorders the traditional power structures in which people traditionally digested information. Throughout history social movements challenge the status-quo power holders; however, Castells argues that digital social networks enable "unfettered deliberation and coordination of action" without the traditional obstacles from the government and media moguls (16). Under this new structure, Castells hypothesizes an increase in social movements fueled by ICT coordination. He extols multimodal, digital networks of horizontal communication as the "fastest and most autonomous, interactive reprogrammable and self-expanding means of communication in history" (15). Hence, Castells argues that these decentralized networks lessen the power of the traditional power holders.

While acknowledging that the Internet is a tool, and thus, open to various utilizations, most cyber-utopians romanticize ICTs as the new pathway to democracy in traditionally closed authoritarian regimes.

On the other side, "cyber-realists" do not romanticize the Web, but understand the limitations of the Internet and the ways in which oppressive regimes can manipulate technologies. "Cyber-realists" argue that ICTs actually strengthen autocrats, who can more easily monitor and neutralize threatening movements and dissidents. Although many scholars are willing to concede the obvious beneficial aspects of the Web, in certain places and times the negative impacts of the Web outweigh its potential power as a democratizing force. "Cyber realists" emphasize the Internet as a tool—open to both good and nefarious purposes. Still though "cyber-realists" hesitate to label the new technological medium as liberalizing. For instance, states are empowered by the Internet's technological advances that create an

unprecedented ability to monitor and analyze massive amounts of data about their own citizens. Especially in authoritarian regimes, such technologies can actually stunt democratic growth in technologically sophisticated ways. Thus, cyber-realists see the Internet as reinforcing authoritarian states' power as opposed to liberalizing impact via the ICTs as posited by cyber-utopians.

In *The Net Delusion: The Dark Side of the Internet*, Evgeny Morozov challenges the idea that Internet favors the oppressed rather than the oppressor (xiii). Morozov cites the stalled Iranian Green Movement in 2009 as an example of cyber-utopianism that naively overemphasized Facebook and Twitter as the impetus for political change. Instead, the Iranian regime shut down the Internet and even used Western technologies to imprison the initial rabble-rousers. More specifically, the Iranian regime employed crowdsourcing techniques to assemble an aggregate of pictures with similar faces and identify individuals involved with protests, leading to their arrests (10). Morozov believes the Internet creates a cyber "Trinity of Authoritarianism"—propaganda, censorship and surveillance—in which networked regimes possess innovative abilities to control their populations powered by the Internet (82).

Morozov acknowledges that the Web can initiate freedom, but in a very limited context. He emphasizes that it is not the Internet that can promote freedom, characterizing such thinking as *internet-centrism*— "[a] pernicious tendency to place Internet technologies before the environment in which they operate—[which] gives policymakers a false sense of comfort, a false hope that by designing a one-size-fits-all technology that destroy whatever firewall it sees, they will also solve the problem of Internet control" (111). Morozov argues that there are two converging lines of thinking: freedom *of* the Internet and freedom *via* the Internet. In this regard, he criticizes U.S. Foreign policy initiatives that promote the Web as illogical. All authoritarian

nations, including China, want information to free flow because they benefit from tracking ICT data of their citizens. Thus, Morozov poses the problem as not access to information, but the ways in which authoritarian regimes use the Web to reinforce their power. In this light, Morozov states that, "most of the firewalls to be destroyed are social and political rather than technological in nature" (111). Towards the end of *The Net Delusion*, Morozov offers the cyber-realist policy maker as the antagonist to the cyber-utopian (318). Instead of thinking in grand terms of whether the Internet undermines or strengthens democracy, the cyber-realist, in Morozov's words, would anticipate that the Internet "is poised to produce different policy outcomes in different environments" (320).

From Larry Diamond's anthology of ICT essays, *Liberation Technology: Social Media and the Struggle for Democracy*, Chapters 2 and 3, respectively titled "Liberation v. Control: the Future of Cyberspace" by Ronald Deibert and Rafal Rohozinskit, and "International Mechanisms of Cyberspace Controls" by Deibert, collectively shed light on the fact that most democratic nations engage in Internet-content filtering. As a result, all global citizens are now subjected to the most surveillance and invasion of personal privacy in history (19). Deibert's argument rests on what he perceives as an all-out blitz on civil society on the Web. Regime type no longer matters, since all nations invoke national security laws to impose broader acts of censorship (25). Moreover, Deibert worries that democracies' rationalizations for such actions only strengthen authoritarian regimes' legitimacy in employing the same technologies, but for perhaps cruder ends (44). This "propagation and diffusion of bad norms" arguably has accelerated with the recent NSA revelations, which simultaneously delegitimize the U.S. government, but also legitimize authoritarian practices of the same sort (44). While some emphasize the growth of

civil society due to the Internet, Deibert raises an alarm that civil societies are under siege by both authoritarian regimes and democracies.

While Deibert reflects upon the ethical implications of democracies legitimizing the use of authoritarian-styled controls like web filtering, Rebecca MacKinnon uncovers networked authoritarian regimes' methods of silencing digital unrest. Specifically, MacKinnon focuses on China's manipulation of its Internet to reinforce its political control. MacKinnon's work shows how the CCP encourages a civil society via ICTs in China, but only to a certain extent. Part of MacKinnon's research highlights the varying tiers of sophisticated technological methods of controlling dissent. In her policy recommendation MacKinnon promotes a "freedom of the Web" sort of argument, which may be seen as vaguely cyber-utopian, or optimistically cyber-realist. She concludes that civil society would grow rapidly in a cyberspace free of Chinese ownership and censorship, and emerge as a much more powerful tool for citizens seeking to hold governments and corporations accountable (XXVII). While her contributions to researching the state control of the Web in China are acutely cyber-realist, MacKinnon's recommendation emphasizes that ICTs are essential to building a more vibrant civil society that will ultimately demand more freedoms and democracy. Again, this reinforces that cyber-utopianism and cyber-realism are not mutually exclusive, but often converge when assessing the liberalizing effects of the Internet.

Interestingly enough, cyber-utopianism faces off against cyber-realism in Chapter 10 of *Liberation Technology*, entitled "Social Media, Dissent, and Iran's Green Movement," written by Mehdi Yahyanejad and Elham Gheytanchi. While paying respect to both Diamond's and Morozov's opposing arguments, the authors write about the successes and shortcomings of the Iranian Green Movement in 2009. Yahyanejad and Gheytanchi view social media as an

important factor in slowly liberalizing Iran. Yet they both realize that ICTs are not nearly as productive as many Westerns initially thought, even going as far as to negate the Iranian Green Movement as a "Twitter Revolution" (150). Thus, at the same time, the authors heed to Morozov's, and cyber-realists largely, argument by conceding the lack of sophisticated social media use on the behalf of the movement, and also sophisticated use of technology by the Iranians to stunt the growth of the demonstrations (151). The authors lament that the civil society built in Iran was not strong enough to mount an actual revolution or extended dissonance. This example also illustrates how cyber-utopianism and cyber-realism interact without being mutually exclusive.

Jonathan Zittrain's 2008 book, *The Future of the Internet and How to Stop it,* acknowledges the catch-22 of technology tools. Morozov's wariness of technology in the hands of authoritarian regimes can be traced back to Zittrain's ideas. For instance Zittrain describes hypothetical nefarious abuses of ICTs to develop sophisticated eavesdropping technology. "They can turn a standard mobile phone into a roving microphone—whether or not it is being used for a call" (4). Most importantly, Zittrain anticipates these uses as beneficial to law enforcement in areas under democratic rule of law, but would be detrimental in "technology-embracing authoritarian states" (5). Thus, Zittrain dismisses the argument as whether the Internet is even "open." Instead, he argues that technology itself is neutral, and neither inherently pro-democratizing nor does it favor the state. As a result, Zittrain's work becomes even more important as democratic states, like the United States, engage in more authoritarian behavior from a formerly "open" source. The collusion between technology makers and states tends to shift the tone of the overall impact of the Internet as a democratizing force to a more skeptical outlook. Therefore, Zittrain predicts the demise of civil society online due to the state's

uninhibited ability to better use the tool of the Internet and ICTs to stunt socio-political movements.

Tim Wu's book, *The Master Switch: the Rise and Fall of Information Empires*, warns against the potential of the Internet as an "open" information arena. Wu does not stress the openness of the Internet in terms of access, but rather in terms of power. Using a historical example of traditional media in the United States during the 20th century, Wu focuses on the monopolization of information and communication technologies like AT&T's (Bell) grasp on telecommunications and NBC's and CBS's domination of radio to emphasize how new technologies are similarly consolidated into conglomerates. Enter the Internet. Wu targets Google, which dominates the information technology market by not producing any content, but rather selling advertisements based on information taken from its search technology (281). Thus, Wu's thesis that new technologies are quickly monopolized and their innovativeness consolidated, thereby defeating the idea that the digital civil society and ICTs create its own content and power. In turn, Wu argues that companies like Google often have more power, and more important power—a deluge of information about its users—, which intelligence agencies crave. Wu also makes an appearance in the PBS *Frontline* documentary, *The United States of Secrets*, in May 2014, in which he critiques the sinister relationship between Silicon Valley technology companies and federal agencies like the NSA.

Recently, several other authors published cyber-realist books in early 2015. Bruce Schneier's book *Data and Goliath: the Hidden Battles to Collect Your Data and Control Your World* argues, "data is the exhaust of the information age" and cautions how data is a by-product of high-tech socialization powered by ICTs (14). Schneier attacks the government and technology companies' justifications for mass collection of data as insufficient compared to the

massive incursion of privacy the all encompassing surveillance imposes. Schneier's argument against mass surveillance as ineffective in stopping terrorist attacks exposes the mislead motives of states to collect data because data is control.

The goal of this thesis is to assess how civil society on the Web in authoritarian regimes and democracies has either shrunk or grown in the context of a post-Snowden world. Grassroots movements in the United States and the Arab Spring resurge the liberalizing potential of ICTs. But even if the revolution will not be tweeted as Malcolm Gladwell declares, it is essential to understand how states use the Web to crush rebellions while constraining the most transformative mode of communication. This thesis seeks to measure how effective the Internet has been at shifting the balance of power in political movements and states. Also, what are the implication of a stunted civil society online via state control of ICTs, as exhibited in China and possibly in the U.S. Lastly, although we consider civil society a pre-condition for democracy and a component of a vibrant democratic society, active societies like terrorist organizations also use the Web to project their ideas and recruit members.

As the literature review demonstrates, the answer is neither clear nor absolute. Cyber-utopianism may be overstated, and much more akin to cyber-realism now than in 2009. The events that have transpired since then, namely the Arab Spring, Occupy Movement, NSA Revelations, state repression, and ISIS, all relied on ICTs to facilitate their respective causes. Ultimately, its not a question of whether the Internet fuels political change, but how political actors use ICTs and whether it empowers individuals and political grassroots movements, or state power. The first chapter seeks to analyze the impact of the state-controlled Web in China. The CCP's domination of the Internet presents a seminal example of how the web can reinforce

state power and entrench state control. I will address the question as to whether a civil society can emerge online in an authoritarian state like China. And if so, to what extent does these online communities group have any source of political legitimacy or acknowledgement from the state.

Chapter Two: Chinese Control of ICTs

China's civil war in the mid-1940s ended with a Communist victory in 1949 led by Mao Zedong against the U.S.-backed Nationalist forces. The relationship between China and the rest of the world became more closed off, especially to capitalist states. In 1989, the protests in Tiananmen Square encouraged the view that democracy had seeped into China. Yet the world watched as the CCP reinforced its power with violent repressive tactics. Many observers believe that a subsequent wave of democratization manifested by ICTs offers a new challenge to the stability of the Party's authoritarian regime. Access to the Internet for large numbers of Chinese citizens opens up a cyber-sphere in which newly formed netizens create, share, and learn information quickly and relatively freely. Websites such as Sina Weibo, a Chinese equivalent of Twitter, revolutionize the manner in which concerned citizens organize and spread communications, and possibly dissent in cyberspace. Therefore, many scholars argue that the Internet can act as a democratizing force, allowing for greater freedom of speech, which will revolutionize the political life of the Chinese and lead to the crumbling of the Chinese Communist Party. However, this is a drastic simplification of the many dynamic forces impacting how the Chinese use ICTs. The history of the Internet in China presents a case study that emphasizes the resiliency of the repressive regime, while offering flashes of a burgeoning civil society online.

In 1994, the first global Internet connection was made in China (Liang, 104). The next year in 1995, the CCP invested heavily in the Internet by building the necessary infrastructure for commercial consumption (MacKinnon, 34). Initially, the Chinese Internet population failed to see expansive growth, only reaching 2 million active members by 1998 (Liang, 105). However, this figure then grew exponentially, reaching 100 million users in 2005 and climbing to 298

million by the end of 2008 (Liang, 105). The capitalist economic reforms beginning in 1978 improved the majority of lives in China and facilitated the use of the Internet for a large number of Chinese citizens. Instead of staving off the Internet and its alleged liberalizing effects, the Party actively invested in the rapid development of telecommunication infrastructure to fund the "Internet boom" in China (Liang, 105). Statistics indicate that in November 2011, there were 457 million Internet users in China, yet by January of 2012, figures showed that the number of netizens had expanded to 513 million (Simpson, 1). Furthermore, these numbers are expected to grow to 650 million, almost half of the Chinese population, by 2015 (Leibold, 1).

The brief overview of the CCP's responsibility in the "Internet boom" and its determination to establish the sovereignty of Chinese cyberspace leads to a more specialized question regarding the Internet as a democratizing instrument. Two distinct and ongoing scholarly arguments debate the unsettled question of the Internet as a democratizing tool. The pro-democracy camp—akin to cyber-utopians—explains that the integration of capitalism would ultimately lead to a gradual democratization from within (Gilley 62). Similarly, this pro-democratic thought believes the integration of the Internet will champion liberalizing principles such as free speech and eventually democracy in a closed, authoritarian China. While the cyber-realist position claims that the Party—in the interest of preserving its power—will do whatever means necessary to stave off the ICTs' liberalizing effects. First, do the Chinese even bother with politics online?

How the Chinese Use ICTs

These statistics illustrate the rapid growth of Chinese Internet users, but now it is important to uncover what most Chinese do on the Web. In a more precise scope, Chinese cyberspace has undergone a "blogging revolution" with a staggering 181 million Chinese users

blogging, according to figures in 2011 (Leibold, 1). By 2011, numbers indicate that Chinese use of microblogs, such as Sina Weibo, increased to over 250 million, signifying the massive popularity of "Twitter equivalents" which serve the purpose of broadcasting information across the large, accessible Chinese Web (Simpson, 1). Consequently, the potential for collective organization and sharing of information is possible with microblogs. Guobin Yang describes the Chinese Internet culture as full of, "humor, play, and irreverence…it is also participatory and contentious" (Yang, 2). Bulletin-board systems (BBS), online communities, and blogs represent the most used tools on the Chinese Internet (Yang, 2). Essentially, Yang argues that the integration of the Internet transforms citizens into netizens by allowing them to relatively freely search through cyberspace and post comments to news articles or public forums on BBS. As a result, Yang concludes that ordinary people are now engaged via the Internet and find meaning and power in their solitary voice over the Web. Yang—in cyber-utopian fashion—reasons that the formation of an online voice transforms into online activism since the instantaneous web facilitates information sharing and organization between other connected Internet users. Furthermore, the Internet allows for public discourse or dissent without *immediate* physical danger. Also, online activists maximize their communicative methods by utilizing mobile Internet to broadcast gathering areas and capture footage more effectively.

The Web Apolitically Strengthens Regime Power

Some may argue that the Internet acts a sanctuary for public discussion since public demonstration is vehemently guarded against as evident in the Tiananmen Square incident in 1989 (Tang, 459). However, (Leibold contrasts with Yang's "rosy assessment of the impact of the blogosphere on Chinese society" (Leibold, 2). Surveys indicate that the, "leading uses of the Internet in China are: search (82%), music (79%), news (77%), instant messaging (77%), and

gaming (67%)" (Leibold, 2). Therefore, the Internet functions more as an "entertainment highway," than as a "information superhighway." Thus, Chinese people are just like their global counterparts and seemingly not very political in their use of the Internet.

The Apolitical Use of the Web Strengthens Regime Power

Other scholars unconvinced by the democratization effect of the Internet explore how the Internet can actually strengthen the Party's grip on power without any censorship methods. Rather the Internet itself entertains the Chinese people and effectively depoliticizes them (Leibold, 3). Furthermore, the Internet, some argue, is an open, unregulated wasteland of rumors and "misinformation" that contribute to a weakening of faith in the liberalizing effects of ICTs (Leibold, 4). The "human-flesh search engines" represent a new form of online activism known as online vigilantism, which targets alleged social offenders to justice by using the power of sharing information on the web (Leibold, 3). However, Leibold argues that it rather leads to a digital form of libel via a "digital scarlet letter" (Leibold, 3). For example, a jealous ex-boyfriend created a weblog in his former girlfriend's name claiming to be an "AIDS-infected prostitute who enjoyed unprotected sex with over 200 clients" (Leibold, 5). As a result, the victim received death threats and lost her job from the outrage of "online lynch mobs," who believed the ex-boyfriend's absurd claims (Leibold, 5). Between the years 2003 and 2007, with the explosion of the Internet and human-flesh search engines, the number of Chinese people who thought the Internet was reliable shrunk from fifty-two percent to twenty-six percent (Leibold, 3).

The burgeoning distrust in the Internet introduces a familiar trend, which Jaron Lanier labels, "digital Maoism," or "the propensity of online collectivism to wreak havoc" (Leibold, 6). Furthermore, these cyber-witch trials can be used against corrupt local Party leaders. In this way the Party can channel these online lynch mobs to expose corruption or abuses of power on a local

level to create a democratic façade thereby legitimizing and strengthening their rule. Some evidence, such as the exploitative use of human-flesh search engines, distracts and divides the Chinese masses. In an ultimate paradox the advent of freedom of speech on the Internet may perpetuate a cycle of fear that is conducive to the self-censorship of dissent. Instead, cyber witch-hunts made possible by the Internet create a new forum of wrongful accusations eerily similar to the Cultural Revolution in the 1960s in China. Regardless, the CCP does not rely on the cyber witch-hunts to protect its rule. Instead the CCP proactively installs measures to contain any liberalizing effects of the Web that may threaten its power.

A Sovereign Chinese Internet

The expansion of the Internet does not simply guarantee the automatic democratization of China nor is it likely that the Internet evolves into a politically charged environment for the newly constituted netizens. Rather, the Chinese Communist Party understands the Internet as a threat to its legitimacy and stability. Despite Internet's democratization effects in China, such as greater opportunity for free speech, the Internet, the Party's control of ICTS will curb any challenge to power. The CCP continuously mitigates the liberalizing impact of the Web by implementing pre-emptive measures, which then enable them to censor their cyberspace to ensure stability and economic growth.

In response to expanding Internet use in Chinese society, the CCP developed technologies to censor and filter politically sensitive data. As stated previously, the CCP itself invested heavily into the Internet to gain economically by connecting to the global network. Essentially, to remain a force in the global marketplace and attract foreign investment to China, its cyber infrastructure had to be constructed. Thus, the CCP appears to be in a catch-22 in developing the Internet for economic purposes, while simultaneously protecting against the

liberalization effects of an open Web that could weaken the stability of the regime. Therefore, the CCP fears foreign influence in the cyberspace and works relentlessly to create a sovereign Chinese Internet.

The "Great Firewall" of China serves the purpose to design a sophisticated control of infrastructure in which the government needs to approve network connections and insulate Chinese ICTs from foreign influence (Liang, 106). Furthermore, the "Great Firewall" filters uncensored information from Chinese citizens, thus making them inaccessible to the rest of the Internet world (Hua, 12). This is possible from the Chinese built fiber-optic infrastructure than enabled ICTs, which allowed the Party to install censoring and filtering mechanisms to sift politically sensitive data. The Great Firewall limits the access to foreign information available to Chinese Internet users; for example, the Firewall blocks terms like "Tiananmen Square" and even "Tahrir Square." The Chinese system censors outside information but allows a flow of information to work through its own native Facebook and Twitter tools, like Sina Weibo and Wechat that produce liberalizing effects by facilitating communication and organization.

Instead of adopting foreign services, the creation of Chinese technology companies ensures compliance with the government's requests for data and strict censorship demands. Moreover, the proliferation of Chinese Internet and technology companies lessens the Party's dependence on Western services like Facebook by implementing Chinese social networking platforms like RenRen and Kaixinwang (MacKinnon, 48). The Chinese Internet companies may at first express concern over the Party's censorship and surveillance requirements, yet the economic monopoly, created by the CCP's aversion to Western influence, allows Chinese companies to service the world's biggest Internet base (MacKinnon, 49). Recent privacy agreement updates in 2012 to the widest used ICT in China, Sina Weibo, bans users from saying

"untrue" statements (OpenNet Initiative). MacKinnon describes this method of ICT control as possible via the "deconstruction of a legal environment legitimizing information control…authorities informal requests to companies for removal of information, technical shutdowns of websites, and computer-network attacks"(MacKinnon article, 43). Again, this manifests the CCP's power in legal department of Chinese technology companies, which creates a sovereign Web dictated and controlled by the Party (OpenNet Initiative). Thus economic freedom does not require "the free flow information," as widely thought by initial pro-Internet pundits that believed economic modernization would simultaneously usher in political democratization. Instead the Party's deep structural design of the Web and its influence over those who produce services and content trade off the liberalizing effects of ICTs for economic profit (MacKinnon, 49).

Networked Authoritarianism: Selective Censorship and Surveillance

However, what is more interesting than a firewall that simply blocks information is how the CCP focuses on stabilizing the online public mood by monitoring what people say (Li, 71). The newfound ability of netizens to comment on media and newspaper's articles compels the CCP to censor any data that it considers "incorrect" (Hua, 3). The CCP employs Internet police that daily monitor and censor politically damaging material and distribute pro-Party propaganda via the "Fifty Centers" (Hua, 13). This censorship agency promotes and nurtures a pro-government viewpoint on the Web. Dissident Internet users label them "the Fifty Centers" because they are paid fifty cents for each pro-government comment and for bashing anti-government comments (Hua, 13). Cheng Hua an anonymous media employee in China considers the CCP's proactive censorship methods as an over-extension and a clear infringement on the Chinese's basic human right to free thought and speech. Like Guobin Yang, Hua exalts the

microblog site, Sina Weibo, which contains some dissenting views of the CCP for all netizens to see (Hua, 13). Hua believes that the presence of dissenting information signifies the Party's inability to censor every 'click' and angry tapping of keyboard. Consequently, they believe such 'relaxed' behavior emphasizes the strength of the Internet in promoting the freedom of speech. Yet, such thinking may be misleading; others speculate that the Internet and its users help the CCP distract and depoliticize the Chinese people. Ultimately the Party is more concerned about collective efforts rather than isolated criticisms on the Web. This could possibly explain the sparse evidence of dissent on Weibo.

Legal Control of ICTs

A special Internet police force was established to aid in the state's Internet surveillance (Liang, 106). Many departments and agencies including the State Council, Ministry of Public Security, Ministry of Culture, and State Secrets Bureau, form a coalition to use and enforce Internet censorship and aid its development (Liang, 108). In 2005, the Chinese bureaucracy published, "Provisions on the Administration of Internet News and Information Services," to justify Internet control and censorship of news organizations by the government in order to "serve socialism and adhere to the correct direction of public opinion" (Hua, 12). Most recently, during the 18th Party Congress in Beijing from November 8-12, 2014, Hu Jintao reinforced the Party's stance on censoring the web by saying, "we [CCP] should strengthen social management of the Internet and promote standardized and orderly network operation" (Ansfield, 2). Over the course of the expansive Internet growth, the CCP provides a copious amount of laws and regulations to legitimize their containment and ownership of the Chinese Internet. An excerpt from the June 8, 2010, White Paper entitled, "The Internet in China," under Section V "Protecting Internet Security" codifies the illegality of any liberalizing effects produced by ICTs:

> The Decision of the National People's Congress Standing Committee on Guarding Internet Security, Regulations on Telecommunications of the People's Republic of China and Measures on the Administration of Internet Information Services stipulate that no organization or individual may produce, duplicate, announce or disseminate information having the following contents: being against the cardinal principles set forth in the Constitution; endangering state security, divulging state secrets, subverting state power and jeopardizing national unification; damaging state honor and interests; instigating ethnic hatred or discrimination and jeopardizing ethnic unity; jeopardizing state religious policy, propagating heretical or superstitious ideas; spreading rumors, disrupting social order and stability; disseminating obscenity, pornography, gambling, violence, brutality and terror or abetting crime; humiliating or slandering others, trespassing on the lawful rights and interests of others; and other contents forbidden by laws and administrative regulations.

Therefore the stern policies articulated by CCP headquarters in Beijing reinforce the Party's steadfast determination to maintain stability and protect economic interests on the Web. As stated previously, the introduction of the Internet was economically necessary for the CCP. Thus, the Party adapted to the liberalization effects of the Internet in China. The Party has contained these "democratizing" effects and limited them to a social platform; however, the CCP uses such innovative technology to censor and manipulate online discourse to stop an opposition movement from challenging their power. Therefore, some believe that the CCP has shifted from classical authoritarianism (pre-Internet) to a networked authoritarianism, or adaptive authoritarianism.

Learning from past experiences, the Party continuously upgrades and sophisticates its tactics in controlling their Internet. Specifically, the CCP employs pre-emptive measures instead of reactive measures to prevent the emergence of any significant online opposition. The 'Great Firewall' method does not depict how brilliantly the CCP handles the democratic power of the Internet. Rather, it is helpful to think of the Chinese Internet controls of censorship, surveillance, and manipulation of information as similar to that of a hydroelectric water-management system (MacKinnon, 37). The managers, or the CCP, have both "routine and crisis management goals:

managing daily flows and distribution on the one and managing droughts and floods on the other" (MacKinnon, 37). Thus from a long-term perspective, the CCP prevents any significant opposition from mobilizing through its daily censorship and monitoring Chinese-controlled micro-blogs. In fact, most recently about half of Sina Weibo has been infiltrated and censored, displaying the effectiveness of CCP's sophisticated censorship technology (Ansfield, 2). In 2010, Wang Chen, head of the CCP's propaganda department and chief of the State Council Information Office reported that "350 million pieces of 'harmful content' had been deleted from the Chinese Internet over the course of one year" (MacKinnon, 39). The CCP realizes the importance of the Internet to the Chinese people and does not completely block all avenues of social media—unless they are foreign sites—thereby emphasizing the CCP's flexibility in maintaining stability. Furthermore, the CCP's ICT management tactics reveals a massive complex system with fluctuating parts that demands flexibility that classic authoritarianism could not accomplish.

No longer does the Party rely on Internet filtering as their sole weapon in Internet control. More sophisticated methods of control are enabled by the traceability of digital data produced by ICTs. Additionally, the CCP launches cyber attacks on dissidents' e-mail accounts to stop the attempted transfer of information to the mainland (MacKinnon article, 39). More sophisticated tactics, include "warrantless surveillance, the creation of 'national cyber-zones,' state-sponsored information campaigns, and direct physical action to silence individuals or groups" (MacKinnon article, 43). In China, classical surveillance evolves into networked surveillance under the CCP's expansive Internet resources. Internet cafes in China must be registered with the CCP and agree to enforce its laws which forbid online gambling and pornographic content (Liang, 113). Frustrated by the growth in the number of Internet cafes, in 2003 the CCP introduced a "chain-

store standard management model" to standardize café procedures in line with CCP Internet protocol (Liang, 114). Such cybercafés require identity registration when logging on a computer, thus emphasizing the meticulous and roundabout manner in which the CCP can track down any excessive criticisms (MacKinnon, 41). Furthermore, the CCP can tap into its constant surveillance online "via its infrastructural and technological equipment and skills" due to its ownership of the Internet 'pipeline' (Liang, 114).

Input Institutions: Party Responsiveness

The White Paper "The Internet in China" was published online from the Information Office of the State Council of the People's Republic of China on June 8, 2010. In section II entitled "Promoting the extensive use of the Internet," the Party document cites how the Party's acceptance of the Internet improves its citizens' lives while reinforcing its legitimacy as responsive to its people, especially in the wake of disaster.

> Soon after earthquakes hit Wenchuan in Sichuan Province and Yushu in Qinghai Province, and a severe drought plagued southwest China, netizens used the Internet to spread disaster relief information, initiate rescue efforts and express sympathy and concern, fully demonstrating the irreplaceable role of the Internet.

Through the Internet, the Party responds to incidences such as a 2001 school explosion in rural Jiangxi Province that the CCP attempted to cover up and compelled the CCP to reveal the truth (Yang, 222). This increased level of transparency produced by ICTs prompts scholars to analyze the impact of public discourse on the Internet and how it affects the news media and erodes Party propaganda imbedded in the news (Yang, 225). The Party itself accepts the growing voices of the people to a certain extent. Therefore, the Party uses surveillance tactics that aims at the head of any opposition movement. Thus, dissidents like Ai Weiwei and other *Democratic* activists receive much more attention and repression than the casual Internet surfing citizen (Ai, xxiii). Ai Weiwei combats the surveillance efforts by exposing his life "in his tweets and blogs, as well

as in interviews and even self-documentaries" (Strafella and Berg, 152). The digital grassroots tools Ai Weiwei developed serves two functions according to Strafella and Berg—to "highlight the absurdity of life under the regime and to spread humanistic compassion" (152). The CCP has no intention to relinquish power; the Internet has actually strengthened its power even more so by integrating digital surveillance and monitoring techniques.

Guobin Yang's book, *The Power of the Internet in China* concedes that the Party continuously refines its "methods of control and governance," thus perceiving the ICT's democratizing effects as constantly countered and squandered (Yang, 222). Yet, Yang sifts through his troublesome findings to proclaim that the most important outcome of the Internet is the establishment of an "unofficial democracy" which creates a social manifestation of democracy within the Chinese Internet (Yang, 223). Although a pro-democracy proponent, Yang recognizes the craftiness of the CCP and their pre-emptive responsiveness in allowing the Internet to satisfy their "immediate social need" without any *political* change (Yang, 225). Therefore, according to Yang, the unofficial democracy created by ICTs is the first step into changing the social and waking the social consciousness of all ICT-connected Chinese of their power, "to speak up, link up and act up against power, corruption, and social justice" (Yang, 225). Yet is this enough to initiate political change?

Input institutions: Democratic Façade

Apart from natural disaster and social responsiveness, ICTs allow the Party to be more responsive to the political demands of the Chinese people, albeit restricted to censorship. Party officials solicit feedback from citizens via "e-parliament" website on policy implementation as well as abuses of power at the local level (MacKinnon, 43). In turn the Party gains legitimacy and presents a democratic façade to its citizens. For average Chinese people ICTs serve as an

input institution that enable considerable freedom to comment on news and post on BBS forums, although they may be censored (Tang, 464). The CCP allows different viewpoints; however, once an Internet user explicitly condemns the Party and attempts to subvert it, the user may face harsh imprisonment if caught. Thus, the CCP encourages Internet users to believe they have a voice individually and not in the form of a political movement. In this spirit, the CCP initiates campaigns to foster a seemingly open political environment. For instance, both Hu Jintao and Wen Jiabao, the President and Premier of the ruling regime in China, hosted online communication with Web surfers via this e-parliament platform in an attempt to utilize the Internet as a transparent tool for citizens to use (Liang, 110). This political stunt legitimizes China's total control of the Internet by making themselves available to the masses via the Web and encouraging interacting online to ensure the collection of all citizens' data.

The freedom to communicate over the Web and the presence of a "social democracy on the Web offers a different perspective than the Western fears of the Chinese Internet as closed and under heavy surveillance. Some believe the presence of the Internet allows activists "to continuously test the limits of such control and quickly exploit any 'structural' weakness (Tang, 469). Yet, the evidence suggests that the CCP has been many steps ahead of those who use the Internet as a democratizing force since the Party relentlessly implements stronger fortifications and mechanisms to contain the liberalizing effects of the Web. Although relations in China have been relaxed considerably with the integration of the Web, they serve as a façade that hides the clear facts that China controls Chinese cyberspace, but selectively targets opposition leaders rather than repressing the entire Internet user population. Thus, the Party's current emphasis on fighting corruption is an ingenious way of enlisting the population in an effort to make the government more accountable and thereby presumably more legitimate. This evolution of

networked authoritarianism shows that China "embraces Internet connectivity not merely as essential for a world-class economic and financial power, but also as necessary form of modern government" (MacKinnon, 28). However, it remains vague how a social democracy can grow into a political entity within the CCP's stringent and omnipresent control of Chinese cyberspace.

These refining techniques of the network authoritarianism reveal the Party's two-pronged approach to containing the liberalizing effects of the Web: it represses dissent while also legitimizing the citizens' perception of the Party, which both together strengthens authoritarian power. The Party combats the liberalizing effects of the Web by constantly upgrading its sophisticated technology to track and eliminate significant challengers. The effects of this two-pronged approach were evident in the suppression of Arab Spring news on Chinese blogs in 2011. In response, the Party detained bloggers using the transcripts from social networking sites to interrogate the digital dissidents (MacKinnon, 42). Thus, the Party's selective use of cyber-attacking prominent members of the dissident opposition and the overall daily propaganda crew that polishes the Internet with superfluous popular support all contribute to limiting the democratizing effects of the Internet.

The Impact of Chinese Internet Policy on other States

Nevertheless, the United States government believes wholeheartedly in the gradual democratization of China impelled by capitalism and its free-market forces, including the Internet. The United States government ideologically opposes the construction of the Chinese Web and Great Firewall because it keeps foreign websites out of the Chinese cyberspace. In 2010, U.S Secretary of State Hilary Clinton's speech, "Internet Freedom," reinforced the United States' formal policy regarding China's closed and censored Internet (MacKinnon, 32). Clinton claimed that "one single, free and open global Internet is an essential prerequisite for freedom

and democracy in the twenty-first century" (MacKinnon, 32). China rebuked Clinton's comments, stating that, "China's management of the Internet is in accordance with the law, and is in line with international practice" (Tzw-Wei, 4). The Chinese foreign ministry spokesman Ma Zhaoxu also lamented that the U.S. disapproval is biased due to their hegemonic motives, "American's intention to claim Internet hegemony" (Tze-Wei, 4). The CCP continues to defend its internal Internet censorship policies with the "White Paper" which declares that Internet control remains "under the jurisdiction of Chinese sovereignty" (Priscilla, 4). Strikingly in hindsight, both the U.S. and China share similar monitoring tactics on the Web to ensure control. The U.S. denounced the "Great Firewall" as anti-democratic, but in practice its intelligence agencies carry out similar operations to surveil electronic metadata collected from its people's ICTs.

In 2014, China held its first world Internet conference in which they called for, "common ground while resolving differences to establish a multilateral, democratic and transparent international Internet governance system" (BBC News China). The highest-ranking Chinese official attending the conference, Vice Premier Ma Kai, emphasized that all countries should severely strike at Internet terrorism activities and work together against cyber-attacks. Contrary to traditional isolationism, it seems as though China now regards its stringent Internet policy as adoptable by other states. William Nee, China Researcher at Amnesty International, warns that Internet freedom is under attack by governments across the world. Nee says, "Now China appears eager to promote its own domestic Internet rules as a model for global regulation…This should send a chill down the spine of anyone that values online freedom" (BBC News China). China's justification of its massive surveillance and censorship is rooted in threats against terrorism, but this is largely illusionary; rather this repressive dragnet is constructed to crush any

sign of mountable dissent to achieve total political control.

Conclusion: Net Effect of ICTs in China

The Party's elaborate control of ICTs is a transferable example of how to manipulate the built-in vulnerabilities and design of the Internet beyond than a generic firewall. The presence of the ICT devices themselves will not usher in an overthrow of the CCP—actual people and political organizations can accomplish such a task. Therefore, it may be completely plausible that many pro-democracy activists hype and exaggerate the impact of the Internet. Regardless of how some Chinese use the Internet, the Party safeguards and controls the Chinese cyberspace to lessen its impact for instrumental change, while simultaneously allowing for much smaller incremental change that provides the Chinese with greater freedoms and presents the mirage of an "unofficial" social democracy. In the long-term the CCP will squash any outwardly threat at the regime, and has laid the groundwork with expansive infrastructure ownership and sophisticated monitoring and pre-emptive tools for eliminating the possibility of pro-democracy opposition groups mobilizing on the Internet in China. In a paradoxical sense, the Internet did bring about liberalization in the sense of greater tools for limited free speech; however, democracy has not taken root in China nor does evidence suggests it will any time soon due to the control of dissent via ICTs. Instead, the Chinese model outlines an effective way to maintain power even while allowing and encouraging use ICTs, thanks to the two-pronged approach that censors harmful information and elicits feedback to construct the perception of a responsive government.

Chapter 3: ISIS' Spinternet: ICT Propaganda

In the following chapter I will investigate how the Islamic State of Syria and the Levant, known as ISIS, harnesses twenty-first century ICTs to broadcast its message in a visual format across the world in hopes of attracting more followers to join the newly christened, seventh century-styled caliphate. Perhaps in emulation of the CCP's elaborate censorship and propaganda efforts, ISIS' own media production team, known as Al-Hayat media center, floods the Internet daily with Hollywood-like productions that range from firing squads, decapitations, counter-Western reporting, evidence of state-building, and youth indoctrination. In order to best understand how ISIS wages this war online, I had to examine this evidence as a primary source, no matter how horrifying and sickening due to the lack of scholarly research in late 2014. Western media companies such as Twitter attempt to censor the gory images posted repeatedly. However, this measure merely censors a small percentage of the graphic posts, and does little to stem the tide of ISIS propaganda online. Once a video uploads to the Internet, third party websites and users can quickly copy and re-disseminate it online. Thus citizens across the world with an Internet connection can access this message through a simple Google search that reveals the same message spawned on a myriad of third-party websites.

That being said, I navigated murky websites, but have found a reliable, scholarly, and most importantly unedited, reposting of ISIS' jihadi videos at www.jihadology.net; a clearinghouse website run by Aaron Zelin, a Richard Borow Fellow at the Washington Institute, Rena and Sami David Fellow at ICSR, and PhD candidate at King's College London. I have categorized ISIS propaganda videos into three different functions: terror, statehood, and international recruitment that defy the cyber-utopian expectations of ICTs as solely liberalizing effects. Like, Neil Postman said, how technology is used by one culture is not necessarily the

only way it could be used (Postman Lecture). Still fledgling, ISIS uses ICTs to help consolidate power. The ICT propaganda arm is akin to role of the Fifty Centers is China, except for ISIS' repugnant content. First, the recent establishment of the Islamic State, known as either ISIS or ISIL, must be explained.

Background and Formation of the Islamic State

In the years following the 2003 Iraq war, ex-Saddam Hussein military leaders, al-Qaeda remnants, and freed prisoners took refuge in the failing state of Syria during its civil war in 2011 (Hubbard and Schmitt). Before 2013 this group identified as another splintered Islamic fundamentalist camp. In June of 2014, its leader and self-proclaimed caliph, Abu Bakr al-Baghdadi announced the creation of the Islamic State along with the seizing Mosul, the second largest Iraqi city. Although still known globally by its original acronym ISIS, or ISIL, meaning the Islamic State of Iraq and Syria, or the Islamic State of Iraq and the Levant, al-Baghdadi refers to the organization as simply the Islamic State, thus emphasizing its expansive, transnational goal, and not limiting itself to Iraq and Syria. For the purposes of this case study, I will refer to the organization by its most well known name, ISIS.

Even though ISIS emerged out of the crippled shell of a mostly defeated Iraqi al-Qaeda, al-Baghdadi runs an organization that by most accounts is more strict and violent than previous incarnations. For example, al-Baghdadi encourages an extermination campaign against religious minorities, like Shiites and Yazidis, which has been denounced by al-Qaeda (Arango and Schmitt). Also, unlike Bin Laden's or al-Zarqawi's al-Qaeda, al-Baghdadi controls an army and wide stretches of land from northern Syria including a long stretch of the Turkish-Syrian border. The reach of ISIS also encompasses virtually all of northern Iraq, stretching as close to 60 miles

from Baghdad. In turn, ISIS has taken on state duties—it does not aspire to be a group hiding in the mountains, rather it wishes to rule captured areas, impose sharia law, and gain legitimacy.

ISIS has benefitted greatly from the Syrian Civil War by capturing state-run oil fields and refineries that finance its operations. It is estimated that ISIS earns between $1-2 million per day from producing oil and selling it across the border in Turkey on the black market (Sanger and Davis). Other estimates project that ISIS can produce roughly 25,000-40,000 barrels of oil per day. As a result, ISIS has quickly become one of the wealthiest terrorist organizations in history.

Like the Taliban, ISIS imposes its version of strict Islamic fundamentalist law in each town and city it conquers. The black flag of the Islamic State is placed in public places to symbolize the legitimacy and rule of the newly formed state. A group of ISIS members from a religious police section in each city ensures that women wear proper attire and that businesses stop for prayer several times a day. ISIS members facilitate market transactions like selling gas and are present at markets. Anyone who defies or is suspected of defying their authority may be subject to public executions or amputations, which are frequently, imposed penalties.

The military component of ISIS ranges from 20,000-31,500 fighters, according to CIA estimates. In addition, ISIS fighters have ransacked Iraqi and Syrian weapon caches, which included U.S. weapons, intended to help Shiites fend off extremist infantry during the 2007 Iraqi conflict. Most alarmingly, 15,000 members of ISIS are foreign-recruited jihadis from Western Europe, North America, and Australia, according to a CIA report largely circulated in Western media in September 2014 (CNN). Through slickly produced video messages and an active social media presence, members of ISIS encourage Muslims across the world to join the fight in the Middle East. Western movement to the region started during the Syrian Civil War to fight against the Assad regime; however, some choose to join ISIS while there. More recently, recruits

travel through Turkey into northern Syria, now an ISIS stronghold. Nevertheless, the military component of ISIS establishes regional credibility through its public executions, which are purposefully captured on film and disseminated on the Internet.

Terrorizing Videos

The ISIS videos proliferating on the Web serve several functions. Decapitation and execution videos aim to illicit public outcry and evoke fear regionally and globally. Other videos narrated by foreign-jihadis depict ISIS as inclusive to attract more foreigners to their cause. Lastly, another type of video functions to imitate and parody Western news organizations by forcing an imprisoned journalist to head the ISIS' news department. All videos include the ominous, waving black flag in a corner of the screen. Most Westerners' visual experience with terrorists consisted of Bin Laden's meager appearance, as he sat cross-legged in a cave with a fuzzy VHS quality picture. To the contrary, ISIS videos are much more slick and meticulously produced. They feature multiple cameras, cameras on drones for aerial shots, sharp graphics, and excellent sound quality. Most importantly, the high-definition resolution creates a familiar viewing experience for Westerners accustomed to digesting similarly glossy television programs and movies. The improved quality of the videos increases the effectiveness of these campaigning videos. ISIS seeks to project a strong image by boasting military victories and demanding hefty ransoms with a knife in their hand. Other videos capture the decapitation of fellow Muslims, known as apostates, those who reject ISIS, or fundamentalist Sunni and Sharia doctrine. These visual messages intend to terrorize and shock, but also to project strength to legitimize its rule as a state, no matter how barbaric. In addition, the glossy depiction of life in the Islamic State seeks to recruit fellow jihadis worldwide to continue to expand the caliphate past the Levant.

ISIS began to draw international attention with the sudden sacking of Iraq's second largest city, Mosul in June 2014. Some parts of the city "warmly welcomed" ISIS and viewed the Iraqi security forces as a hostile Shi'a militia. In under a week, only 800 ISIS militants forced the Iraqi army to flee (Frontline). ISIS videos show the explicit killings of captured Iraqi security forces. The next month, ISIS posted videos of roughly fifty Syrian soldiers killed in battle and some beheaded on July 25 in Raqqa (Al-Jazeera).

In response to the repeated violations of Iraqi sovereignty, President Obama launched an airstrike campaign to ultimately "destroy and degrade" the ISIS threat. International attention grew fervent in the summer of 2014, when ISIS, in reply, began launching jihadi videos with the help of its propaganda machine, the Al Hayat media center. These videos threatened to kill Western journalists if U.S. led airstrikes in the area did not cease.

First Function: ICT Killings

Captured in northwestern Syria in the Fall 2012, journalist James Foley appeared in an orange jumpsuit in the desert in an ISIS beheading video. Foley showed little emotion and stoically stood on his knees while an English-speaking ISIS member decried U.S. involvement in the area. Unlike previous terrorist videos, ISIS invests time and money into high-definition equipment and a production team to produce a video with stunning effects. The audio is remarkably clear with multiple microphones. Visually the endless desert beyond the foreground is especially scenic. The British-accented ISIS executioner has been nicknamed "John" by his hostages, and the Western media gave him the nickname, "Jihad John" (UK Daily Mail). While speaking, he wields a long blade knife. Once he attributes blame for Foley's death squarely on the United States, Jihad John begins the decapitation process as the camera zooms in on Foley's neck and quivering body. Then, there is a cut-scene and the entire execution is avoided, an

interesting decision of self-censoring. By making the video less gruesome, ISIS hopes more people will be able to access it. The camera slowly comes back into focus and pans to Foley stretched out on the ground with his head on his stomach. The high degree of orchestrated control of this video reflects ISIS' desire to gain legitimacy via ICTs.

The second video featuring Steven Sotloff begins with a fuzzy picture of an Obama speech artistically embedded in the video, another characteristic of a sophisticated production team. Here, ISIS clearly attributes the execution deaths to U.S. foreign policy. The vast desert in the foreground attempts to depict ISIS as standing out in the open and unafraid of retaliation. The distinct differences reinforce the message ISIS wants to project their strength. More importantly, these types of stylistic effects are more digestible for the HBO-watching American public. For once, a terrorist organization caters to the stylistic appetites of the West by imitating their entertainment, albeit in a chilling manner. These artistic qualities mix oddly with the horrific message being played out on the screen that projects strength and perhaps appeals to Western culture in hopes of recruiting more jihadis.

Aside from the widely publicized beheadings foreigners like Foley and Sotloff, ISIS regularly uploads public executions and beheadings. They label these videos as killing religious apostates, indicating that ISIS kills fellow Muslims more frequently than foreign prisoners. One such heading reads, "Liquidating One of the Apostates Who Betrayed the Mujahidin," "Soldiers of the Nusayris in the Hands of the Islamic State" and "Harvest of the Apostates" (jihadology.net). These videos are more brutal than the execution videos geared towards the Western audience. A crowd of ISIS fighters imposingly stands behind the executioner, or sometimes, they stage the killings in a public square or street. Here, ISIS projects their strength

to the communities in which they rule. They legitimize themselves through the sword, and extinguish opposition, or deviant religious groups through public execution.

The most recent, and most horrifying, video depicts the captured Jordanian pilot caged and burned alive. The scene is well staged and the camera pans to reveal a gasoline drizzle that leads past a tunnel of IS soldiers into the cage with the prisoner. The fuse line is lit and the fire engulfs the line and moves into the cell. The camera unabashedly captures the pilot's excruciating death. Even worse, ISIS broadcasted this video on high-definition screens throughout its strongholds. In Raqqa, citizens gathered around to watch the execution. This is a purposeful campaign to legitimize their rule via strength and fear transmitted by ICTs.

The Second Function of ISIS' videos: Imitation Games

First debuting on YouTube on September 18, 2014, former British journalist and current ISIS detainee John Cantlie begun a video series entitled "Lend Me Your Ears" to offer a critique of Western media and a more "accurate" depiction of events in ISIS. Unlike his fellow prisoners who lost their lives in a horrifying decapitation, Cantlie's life has been spared. Naturally, Cantlie acknowledges how his work may appear feigned since he is beholden to ISIS by a gun. Nevertheless, he claims that since his government abandoned him, he has nothing to lose and thus contributes as the informal Western ISIS journalist. Yet Cantlie never explains specifically why his life has been temporarily saved to be the main reporter behind this series. Instead Cantlie in his Western-trained broadcast style offers a counter-balance to the dominant Western media:

> I am going to show you the truth and systems and motivations of the Islamic State, and how the Western media, the very organization I used to work for, can twist and manipulate that truth for the public back home. There are two sides to every story. Think you're getting the whole picture? (Lend Me Your Ears, Introduction Video).

Then Cantlie alludes to how other nations have secured the release of ISIS detainees by negotiation, and criticizes the United States and Britain, which have refused to negotiate. This

deprecating commentary is the result of a concentrated propaganda effort to produce and control a grand ISIS narrative that pits the hegemonic world powers against a small group of fearless jihadis. ICTs are the mode through which this propaganda disseminates.

Donning an orange jumpsuit and appearing gaunt with spotty facial hair, Cantlie does not yet look the part of a credible journalist. However, his bluntly honest delivery conveys sincerity to the viewer. At this point Cantlie promises further videos, but the message is not as effective since he admits his status as a prisoner and looks the part. However, this video sets the stage for an onslaught of ISIS propaganda in the style of Western media, with John Cantlie emerging as the Western mujahedeen spokesperson. The series' ironic title "Lend Me Your Ears" alludes to the Shakespearean play, *Julius Caesar*. In Mark Antony's oration, he attempts to justify the actions of Brutus and the assassins by "coming to bury Caesar, not praise him." Yet by the end of the speech the crowd turns against the conspirators and mourns Caesar. Similarly, Cantlie appears before the camera to shift the international community's attention against the West and legitimize ISIS. Hence, this series of videos is clearly distinct from gruesome decapitation clips and only improves in its quality and rhetoric.

In his second video of the "Lend me Your Ears" series, Cantlie responds to President Obama's September 2014 speech commemorating the 9/11 attacks and outlining the plan to defeat ISIS. Cantlie likens U.S. involvement in the areas as the third reiteration of the Gulf War and doubts the effectiveness of a "boots-on-the-ground" strategy led by Iraqi forces in taking back ISIS-controlled villages and cities. Cantlie's delivery is strong and effective, and he quotes *New York Times* journalist Peter Baker, who describes the impending conflict as one of the "bloodiest, most vicious fratricidal conflicts" (YouTube). Cantlie attacks President Obama's credibility in running a war against the Islamic State. His message strongly alludes to the first

two arrogant wars in the Middle East and how American behavior has failed to learn from those experiences. Cantlie's rhetoric is not simply pro-ISIS propaganda, but more akin to an anti-war effort. Thus, the effectiveness of the messages channeled through Cantlie as a Western journalist is devoid of violence or ISIS atrocities, and rather focuses on a more rational viewpoint that may resonate with liberal-minded Westerners. Here, ISIS effectively harnesses the power of video-sharing sites to reach an audience willing to click on a video—initially out of concern for Cantlie, but then perhaps becoming more sympathetic as a result of watching the "Lend Me Your Ears" series.

In episode four, Cantlie again sets out to counter Western media that promotes another "unwinnable" war in the Middle East. Again, Cantlie sits in his orange jumpsuit with a black backdrop and appeals to the indifference of the Western population that is more concerned about the economy than another drawn-out war in the Middle East.

> They say that people have short memories, but the ink has not even yet dried on the written orders to pull out of Afghanistan. Yet here we are gearing up for Gulf War 3…and another complex geo-political war in a far away country, that does not concern them, is of little interest. And yet at the first sniff of something they don't like, the American war-machine springs to life, whipped along by the Western media as usual.

Cantlie cites the August 7th decision by Obama to launch airstrikes as opportunistic. The justification for protecting religious minorities, specifically, the Yazidis, is inconsistent with U.S.' refusal to intervene in other grave crimes like, the Assad regime's use of chemical weapons in August 2013, argues Cantlie. The video production is improved in this video with pans to pictures that reinforce Cantlie's message, like a row of white-wrapped corpses from a recent airstrike. Episode four's overall propagandist message digs at the futility of the two failed wars and condemns the Western media for whipping up support for another unwinnable, costly war.

Episode 5, broadcasted on November 2, 2014, begins with the usual refrain from Cantlie, describing himself as "the British citizen abandoned by my own government and a prisoner of the Islamic State for nearly two years." Cantlie addresses the executions of his peer journalists by first emphasizing that the community of prisoners was treated well and that "it wasn't a bad life." Cantlie remarks how Spanish and French journalists were freed when their governments met certain conditions. Cantlie cites e-mails from American families and explains how the U.S. government did "absolutely nothing" to secure the release of its citizen-journalists. Cantlie argues that the mujahedeen have repeatedly said that Western governments do not care about us.

Episode 6 continues the narrative of the forgotten journalists and elaborates on the failed rescue attempt by U.S. forces on July 4, 2014. Cantlie laments that the recent exchange of prisoners to secure one U.S. soldier, Bowe Berghdal, is deemed more important than saving six civilians. Cantlie says "they were left to die" due to the government's refusal to negotiate their release. The overall message of the video is that their lives were politically expendable and their governments abandoned them, and then used their executions as a means to launch the coalition. Cantlie forcefully states, "I will continue to speak out against this military action and the deceitful arrogance of these governments for as long as the mujahedeen allow me to live."

Although Cantlie's rhetoric is well written and rehearsed, these videos do not best utilize his skills as a Western media correspondent, until he appears in three media-styled reports in Mosul, Kobane, and Halab. The Al-Hayat media center precisely imitates the style of Western programs, like CNN, creating a production that uses high-definition quality and graphics. Cantlie's reports feature him walking through cities controlled by ISIS. In one episode entitled "Inside Halab" Cantlie walks among the rubble, but emphasizes the prosperity of the city due to ISIS control in a twelve-minute slickly produced segment: "Driving into Halab, one can truly

appreciate, firsthand, the huge swaths of land liberated and controlled by the mujahidin" (Al-Hayat Media Center). These comments, along with the cable-new graphics, are ISIS' attempts to prove its statehood. It does not see itself as merely an organization, but as a state that holds territory and performs state function. In the middle of the segment, Cantlie acts like a war-reporter, insisting that drones had just bombed a market. Although it is difficult to authenticate the footage, the marketplace does look damaged—but that could have been staged. Nevertheless, Cantlie describes the pandemonium and runs to cover. In these reports, ISIS directs ICTs as a persuasive force to legitimize their rule and mollify it through Cantile's voice to the global audience.

Lastly, ISIS uses its video production team to exhort its "humanitarian" and state actions to the regional. One video shows construction equipment paving over dirt to re-make a road ("Services Authority: Repairing and Opening a Road in the Village of al-'Abbāsīyyah – Wilāyat al-Khayr"). Another video boasts the new school curriculum imposed by the Islamic State, yet all the students are boys indicating the suppression of girls' rights to receive an education ("Reopening Schools with the New Curriculum – Wilāyat al-Khayr"). These videos attempt to counter the Western impression of the Islamic State as a tyrannical rule. By showing humane conditions, ISIS seeks to legitimize their rule to the surrounding area by broadcasting such videos only in Arabic.

The Third Function of ISIS' Videos: International Recruitment

Like grassroots movements augmented by the power ICTs, ISIS' propaganda department harnesses the Web to blast its messages, both violent and informative, across the world in hopes of recruiting more followers to commit Jihad in the Levant and the West. ISIS has gained the attention of Western governments and the people of these nations who have heeded the call.

Attacks in Ottawa, and Paris were influenced by ISIS propaganda facilitated by Jihadi postings on the Web.

On January 10, 2015, the Islamic State released a collection of memoir-styled videos of one of the French gunman, Amedy Coulibaly. Sitting underneath the ISIS' black flag and a weapon by his side, Coulibaly dons militant fatigues while pledging his allegiance and devotion to ISIS. The publication of these posthumous videos signifies the effectiveness of the ISIS' media in recruiting followers who not only perpetrate acts of violence, but carefully document their devotion to the ISIS cause before the suicidal mission.

In October 2014 two separate lone wolf attacks terrorized Ottawa and Canada. Prime Minister Stephen Harper emphasized that although the attacks were separate, they were both inspired by ISIS (CBC News). After the attacks a Canadian ISIS member, John Maguire, encouraged more lone-wolf styled attacks in his home country (ISIS video). In another jihadi video, another Canadian Andrè Poulin mentioned that he played hockey as child growing up in Canada, but ultimately heeded the call to fight for ISIS (CBC News). While in the U.S., ISIS members have also turned up in the Middle East yet no U.S. citizen has executed an ISIS sponsored attack on U.S. soil. However, thirty-three-year-old Douglas McAuthur McCain traveled to Syria to fight for ISIS and died in action (Washington Post). This marks the first known American citizen killed fighting for ISIS. In his social media history McCain expressed violent thoughts and sincere interest in joining ISIS:

> "The 'soldiers of Allah' are 'coming back." "I will be joining you guys soon." "I'm with brothers now," "It takes a warrior to understand a warrior. Pray for ISIS."

Individual actors, like McCain, frighten Western nations not just because they flee to the Middle East and fight for ISIS, but because they have the passport to return domestically, there is a

greater potential for a domestic terrorist attack. Although McCain converted to Islam years before he went to fight for ISIS, he became radicalized by trips abroad and expressed his jihadi beliefs on social media. Again, this fact reiterates that ICTs have no ideological preference since they are tools.

Many other stories have emerged of young people attempting to join ISIS. 19-year-old Mohammed Hamzah Khan was caught trying to flee to for ISIS ground via Istanbul with his younger brother and sister. Authorities charged Khan with "attempting to provide material support to a foreign terrorist organization," (Washington Post). The Khan siblings had been persuaded to join ISIS through twitter exchanges with members. More shocking, the Khan daughter tweeted ISIS propaganda documentaries that featured gruesome violence and decapitations (Washington Post). Some have labeled this "bedroom jihad," ISIS propaganda disseminated on the Web that targets young people to join their cause. All one needs is an Internet connection facilitated through a computer, or a smart phone to become attracted to the message echoed by newly converted Western jihadis fighting in the Levant. U.S. authorities detained, "at least 15 U.S. citizens—nine of them female" who attempted to join ISIS (Washington Post). This larger trend concerns Western governments who have enhanced efforts to monitor suspicious flying activity, especially those traveling to Turkey, the unofficial front door to the ISIS ranks.

Similarly, the U.K. faces a more pronounced "bedroom jihad" threat due the significant Muslim population in England. ISIS propaganda videos hope to attract more fighters for their cause. In order to stop the flood of British Muslims fleeing to fight, the British government set up a new program, "Prevent", to counter the Internet radicalization of its citizens. Sir Peter Fahy expresses concern over ICTs:

> I think the big concern about the current situation is just a huge amount of material[,] which is available on social media, in the various publications and the various videos… You've got, you know, a person who's identifiably British who's gone out there and is absolutely using social media to be able to communicate directly into your son or daughter's bedroom…

The increased perceived threat by ICTs warrants the intrusion of the mass collection of ICT data in the United States and Britain. Like China, the effects of ICTs—whether democratizing, or not—are potentially destabilizing. However, the Western recourse for dealing with these problems is to control more data; a technological fix that is not applicable to this situation. ICTs are not fallible because they are tools. There are ways to counter youth disillusionment that tackle the core, socio-political grievances; expanding an already invasive electronic dragnet ignores the root, societal problems.

ISIS on Twitter: Western Intelligence Agencies' Response

After Fahy's outcry on "60 Minutes," Robert Hannigan, the head of the British intelligence surveillance agency GCHQ, attributed blame to Western media companies for enabling the spreading of ISIS propaganda through their social media services. Hannigan correctly addresses the difference between ISIS and al-Qaeda in which the former uses the "web as a noisy channel in which to promote itself and radicalize new recruits," and the latter lurked in the dark spaces of the Internet without massive digital mobilization (Hannigan's Open Letter). For instance, ISIS commonly hijacks popular twitter hash tags like #WorldCup2014 to get their message to a much wider audience rather than disseminating material in the dark, less-populated web. However, Hannigan does not realize that Twitter, a technological medium that is open to both positive and nefarious uses, cannot control what its user say, especially several thousands of them. Hannigan does not understand the problem that ISIS "bedroom jihad" propaganda is nearly unstoppable due to the myriad of third-party sites that launch their message via ICTs. As Lessig

notes, there is tradeoff, or compromise when allowing technologies to flourish since dissidents in authoritarian nations can use them, but also can "Al-Qaeda" (Lessig, 225). To adapt the quote this study, so can ISIS harness the power of ICTs to control its image to evoke fear and earn legitimacy as a means of consolidating power.

Nevertheless, Twitter and other companies understand the real-world implication of graphic tweets and suspend ISIS-supporting accounts in violation of its terms of service. Yet Twitter faces logistical challenges in banning accounts at the same pace they are recreated. From September to December 2014, Twitter suspended a minimum for 1000 ISIS-supporting accounts that yielded high traffic (Brookings Research). Yet, during this period, Berger estimates that ISIS supporters used at least 46,000 Twitter accounts (Brookings). In 2011, ISIS affiliates began creating accounts, totaling only 1,064 (Brookings). In 2012 the accounts created figure increased to 2,380 and almost doubled in 2013 to 4,378. In 2014 the number of pro-ISIS Twitter accounts rose astronomically to 11,902, as the group became more infamously known. The Tweets per day figures explain how despite a finite amount of accounts, ISIS supporters blast Twitter with "concentrated bursts of high volume" that establishes a digital presence on social networking sites (Brookings). The brazen presence of ISIS on Twitter debunks the cyber-utopian view of ICTs, which includes social networking sites, as innately pro-democratizing. Rather, the ISIS example proves that people and culture shape how technology is used. ISIS uses Twitter to gain global consciousness and attract followers via its fast-acting, digital propaganda apparatus, a feat that was impossible before the emergence of ICTs.

Yet some cyber activists, ranging from individuals to the cyber-hacktivist group, Anonymous, survey Twitter for pro-ISIS Twitter accounts to report to Twitter for suspension. One activist, XRSone, released a roster of 26,382 accounts to be deactivated by Twitter

(Gladstone). Additionally, J.M. Berger, who analyzes ISIS' Twitter use, doubts the effectiveness of such lists (Gladstone). Due to the anonymity of the Web, it is difficult to pinpoint the number of pro-ISIS accounts, but the scholarly estimate ranges from 46,000 to 70,000. Recently, the *New York Times* estimates that the vast ISIS' network carries roughly 500 million messages a day in various languages (Gladstone). Almost one in five ISIS supporters on Twitter are English-speaking, whereas three quarters select Arabic (Brookings).

Hannigan laments the growing encryption procedures used by Western technology companies that he says enables ISIS to communicate easier and without being identified. After the Edward Snowden NSA revelations, the Western public lobbied for better encryption tools to protect their privacy and communications against pervasive surveillance intelligence agencies, not to protect a small portion of terrorists. Again, the innate design of ICTs as a tool allows the equal potential for a vibrant digital civil society, or terrorist propaganda. Here, Hannigan wrongly accuses such innovations, labeled "Snowden approved," as detrimental to the counter-terrorism effort and even enabling and perpetuating ISIS' online reach (Hannigan's Open Letter). Hannigan essentially claims that improving privacy is directly correlated to enabling ISIS operatives to enjoy the same benefits that facilitate terrorist missions and international recruitment. Again framing the problem of ISIS' use of ICTs as the problem of technology companies ignores that ICTs are tools, open to both good and nefarious purposes. Steps can be made to eliminate pro-ISIS tweets; however, the proposed de-encryption of devices affects all users, not just the fraction that use anonymity to design attacks.

Conclusion

To use Morozov's term, ISIS created a "Spinternet"—a Web with little censorship but lots of spin and propaganda that reinforces their ideological supremacy as a byproduct of open-

ended nature of the Web (117). The Islamic State artfully uses sophisticated equipment to create visual productions and disseminates them using the power of the Web, not solely Western social media companies. ISIS lacks the censorship and surveillance techniques, and rather utilizes ICTs as a Spinternet as evident in the rampant pro-ISIS tweets. Additionally, the video messages range enormously; from gruesome decapitations to state building exercises to a Western British accent reporting in a pro-ISIS slant in major cities. Yet all of these ICT examples function to propagate and reinforce its newfound power. ISIS is revolutionary because they are the first group to successfully harness the diverse uses of media and advance their multi-faceted agenda. ISIS physically launched an ground campaign with remarkable success; however, it can be argued that the Islamic State has successfully infiltrated the bedrooms of perhaps disillusioned Western youth and convinced them to abandon their Western comforts for a life governed by sharia law and on the frontlines of an intensifying religious-political war. In this context, the costs of ICTs allows for like-minded individuals, irrespective of their ideology, to connect and share ghastly videos. Unlike the repression of ICTs in China, in self-governing areas like ISIS, it is difficult for foreign nations, like Britain, to control how ICTs are used. However, it is certain that ISIS controls and increases its image via ICTs.

Chapter 4: Egyptian Grassroots ICTs and State Repression

Two transformative events powered by technology in 2011—the Arab Spring and Occupy Wall Street. Accordingly, *Time* Magazine named the Person of the Year "The Protestor." In 2015's hindsight, what is the legacy of these movements, and how has technology evolved in similar and different political settings?

Grassroots Mobilization

In 2011, the Arab Spring uprisings consisted of spontaneous popular mass movements, which opposed traditional dictatorships ranging from North Africa through the Middle East. Although the roots of the unrest lie in Tunisia, the focus of this chapter is on Egypt's grassroots mobilization online and in the streets that forced President Hosni Mubarak to resign. The date January 25, 2011, resonates in the minds of Egyptians as the start of the mass protests. Hundreds of thousands of protestors packed Tahrir Square, a sight resembling the mass demonstrations in Tiananmen Square in China in 1989. Unlike that example, political activists in Egypt were equipped with ICTs that facilitated the mass mobilization that eventually forced Mubarak to step down from power.

How much of a role did ICTs play in the uprising; was this a technological revolution? And, four years later, how has Egypt changed since the initial emergence of political change?

Is Egypt different than Iran?

In 2010, Evgeny Morozov scoffed at the notion of the supposed democratizing power of the Web by marshaling evidence of how authoritarian regimes coopt the web into a more sophisticated power apparatus. The failed Green Movement in Iran in 2009 was his introductory example of what he called cyber-utopianism; an unrealistic and naïve belief in the ability of the Internet and social media to impact political power. In addition, the Chinese example fits

Morozov's model as a state that failed to sufficiently liberalize with the advent of the Web. The CCP presides over a local democratic façade of the Internet, while strictly forbidding any threat to its power through an overbearing censorship task force that suppresses negative comments. However, the uprisings in Egypt in 2011 present a formidable challenge to Morozov's criticisms of cyber-utopianism, as social protest powered through traditional and Internet-enabled methods of organizing led to political change.

ICTs: are they Weapons of the Weak?

In Manuel Castells' book *Networks of Outrage and Hope: Social Movements in the Internet Age*, a heightened importance is placed on the development of ICTs and how it improves the protest capabilities of the politically weak. More specifically, Castells cites the infrastructure of the Internet as a revolutionizing form of horizontal communication that does not rely on traditional vertical forms of communication made possible by media moguls (15). As a result, the Internet gives birth to the idea of mass self-communication: "the use of the Internet and wireless networks as platforms of digital communication" (6). This mass self-communication development provides "the technological platform for the construction of the autonomy of the social actor, be it individual or collective vis-à-vis the institutions of society" (7). According to Castells, "This is why governments are afraid of the Internet…" this sort of communication cannot be physically tracked or predicted as it were before the digital age (7). Indeed, the Mubarak regime was caught off-guard by the savvy use of technology, and perhaps regrettably miscalculated the power of ICTs in organizing more widely attended protests. The political prowess exhibited by the combination of ICTs paired with a disgruntled citizenry poses a threat to authoritarian regimes with and without a democratic history; however, going forward, these

repressive crackdowns on ICTs and in the street incentivize authoritarian responses, and debatably encourage a wave of control rather than granting liberalizing freedoms.

An Internet Revolution?

Political unrest began between January 17th and 20th when at least five Egyptians attempted self-immolation in front of public buildings in Cairo (Middle East in Focus, 354). Shortly after, an organized social media presence prepared for a nationwide day of protest on January 25th (Middle East in Focus, 354). The spirit of the Arab Spring inspired millions of Egyptians to protest in the streets and call for the resignation of President Mubarak in Cairo's Tahrir Square but also throughout the country. On January 28th, Mubarak's government disconnected the nation from the Internet in hopes of quelling unrest triggered by social media organizing (Howard 21). Despite the outage, the protests persisted while Egypt's economy and government agencies' productivity tumbled due to the loss of Internet access from the four-day blackout. Mubarak's plan called for deliberate chaos; he ordered ATMs and stores to not be resupplied while arranging curfews (Middle East in Focus, 356). In order to restore order and re-legitimize his rule, Mubarak deployed prisoners and thugs to thwart the protesters (356). Yet, despite several attempted compromises, including dissolving his cabinet and agreeing to not run for reelection, Mubarak at last relinquished power on February 11, 2011, which eventually set the course for democratic elections in the next few months.

The Arab Spring in Egypt spread more quickly with a wide base of mobile phone users and the facilitation of online networking that could rapidly organize masses of people in public spaces. Philip Howard and Muzammil Hussain argue that nations without this "civil society with digital scaffolding are much less likely to experience popular movements for democracy than are countries with such an infrastructure" (123). Howard characterizes this moment as Democracy's

Fourth Wave in accordance with Samuel Huntington's democracy wave theory. Digital tools alter the balance of power between the authoritarian regime and its citizens, yet unfortunately it mostly sways to the benefit of the regime in power. The hardened military rule established in the wake of Mubarak questions ICT effectiveness.

Pre-2011: Constructing a Digital Civil Society

In his introduction to *The Digital Origins of Dictatorship and Democracy* (2010), Howard forebodingly investigates how the Internet mixes with the Muslim world, socially and politically. With lowering economic costs, the mass use of the Internet is affordable and easily accessible at home, work, and public libraries and cyber cafes (31). ICTs in Howard's words, "enable both the production and consumption of political culture" and disseminate communications between networks (31). Another reason for mass adoption of the Internet is that governments, like China, invest into Internet infrastructure to encourage business modernization. To avoid modernization for fear of digital reprisal was a key concern in China, which the party dealt with by owning the physical ICT infrastructure. In Egypt, however, much of the infrastructure of the Internet was provided by Western companies. From the outset, Egypt never had full control of what would later turn out to be a major liberalizing force. Lastly, Howard cites the Internet as a convenient information technology to discuss culture, politics and share grievances and aspirations (32). In Egypt this phenomenon is best supported by the surge of the Egyptian blogosphere. Moreover, combined with this willingness to contribute to once improper behavior—to discuss and question government—the Internet acts as "crucial democratic information infrastructure" that dramatically empowers a citizen with an internet-connected smart phone that can share information rapidly and widely (Howard *Digital Origins*, 108). This is when Egyptian citizens become "citizen-journalist" at the point when they can reach out to

other concerned citizens and share views and evidence of governmental corruption (Howard, 112). Out of these early channels a mass consensus grew amongst digitally connected Egyptians.

In opposition to this optimism, Howard stresses how even more democratic nations contract security services to harass bloggers, since they raise collective consciousness with breaking news stories and pictures and videos as objective evidence (Howard *Digital Origins*, 117). Before the Arab Spring, Egypt already boasted a record of imprisoning bloggers, by identifying them as political oppressors (Howard, 117). Howard dutifully notes the changing attitudes of the public towards the Internet as a news-source that is more reliable than traditional information gathering like state-backed print, television and radio-mass media (129). "Even though a particular autocratic state may not have the tradition of free speech or strong legal institutions for promoting such conduct, new media technologies are serving the conduit for cultural content that promotes such values" (129). Contrary to state-media, ICTs' counter establishment nature challenges the political insufficiencies of traditional types of less dynamic media.

Information Infrastructure

In chapter 5, "Civil Society and System of Political Communication," Howard describes the Internet as an "invaluable logistical tool for organization and communication for civil society groups" and lauds its information infrastructure independent of the state (132). Online bulletin boards and chat rooms exercise virtual free speech in typically authoritarian Muslim nations (133). Howard enriches his definition of civil society, "as a crucial part of all democracies" and as "constituted by a plurality of groups representing diverse perspectives and promoting those perspectives through communications media and cultural institutions" (133). The falling costs of Internet access explain how civil society grows rapidly online (140). "Internet access has vastly

improved the quality and quantity of informational resources available in public and national libraries" (144). Howard makes the prophetic statement that the Web does not only contain civic activism, popular protest, and political opposition, "but that the Internet is the means by which social movements have formed" (146). ICTs undoubtedly improve the cohesion and impact of social movements compared to an earlier, pre-ICT era (147). Castells similarly underlines Howard and Hussain's emphasis on digital networks that facilitated civic leaders' protests (104). Castells argues that what makes the Arab Spring unique is its spontaneous non-traditional mobilization separate from formal organizations, which had been delegitimized in the eyes of the young participants by self-censorship and suppression during the Mubarak years (106).

Democratization Theory—Technology Diffusion

These points aggregated from Howard's pre-Arab Spring book clearly identify the growth in civil society thanks to technology diffusion. In 2013, Howard and Hussain determine ICTs as a causal role in the sociopolitical movements, and as a vital in the Egyptian example. Still, Howard concedes that there is a dark side of the Web—"video clips of bombings, beheadings, [on the Internet]"—without quantifying the effects this may have on the causal role of netizens who may be more hesitant to post and share information once the government responds brutally, as in the case in Iran in 2009 (134). Also, Howard recognizes the authoritarian regime's own digital tools to constrain and crush digital dissent with censorship and pursuit of a "cultural management" agenda (135 and 147). Yet, what this critique does not account for is the assumed automatic politicization of users on the Web and the cumulative impact of relentless authoritarian pressure that results in a pacified citizenry online and off. Howard devotes many pages to describing censorship methods and the multiple choke points and filtering options of the information networks (171). Yet this sort of digital repression works against ICTs in the long run

since ICTs generate data-tracking information that helps the regime detain and suppress bloggers. While Mubarak was being overthrown, fear in Egypt temporarily subsided until the military's use of digital and physical repression re-evoked fear that in turn minimized the liberalizing effects of ICTs.

Digital Dissent

Before the Arab Spring could take place, an alternate space of dissent was created online for netizens under non-democratic regimes, like Egypt's. Yet, Howard concedes that increased political communication does not necessarily translate into governments transitioning into democracy immediately, like Egypt (195). Rather this digital transition lessens the authoritarian sting allegedly; Mubarak stepped down, and Morsi too, crumbled under popular pressure and military interference. Howard's reasoning is logical—although citizens are not yet at the ballot boxes—a robust online discourse of politics increases the political consciousness in nations accustomed to limited public discussion. Over time, citizens can extract limited concessions from wary authoritarian regimes. After Mubarak, the opening of the political sphere led to an increased popularity for once "illegal" political groups, like the Muslim Brotherhood (195).

As Howard states, the Web provided an autonomous and anonymous space unparalleled in Egyptian civil discourse. As I alluded to in the first chapter, Howard labels the burgeoning social media sites online as the digital scaffolding in which civil society can grow online (44). Castells similarly remarks that, "[the] Internet and mobile phone networks are not simply tools, but organizational forms, cultural expression and specific platforms for political autonomy" (103). Even under government censorship, Egyptian bloggers used the platform of the web to vocalize their grievances online. More importantly, these dissidents enjoyed the anonymity of the web that created "alternate newscasts and building spaces" where publication of such dissent is

not attached to any actual name (Howard and Hussain *Democracy's Fourth Wave*, 38). Howard argues that in this digital realm a civil society emerged to debate contentious issues that were not allowed in the public square (38). Thus, the Internet social networks converged with the urban networks at the crossroads of symbolic public power, in the squares for open protest (Castells, 81).

To avoid IP tracking, the servers for these websites were located outside the jurisdiction of Egypt and thus could not be taken down, unless all Internet communications were disconnected. An active online civil society, Howard boldly claims, "is both a necessary and sufficient cause of transitions out of authoritarianism" (197). It follows then that with technological diffusion, a vibrant virtual space can achieve political outcomes (198). Irrespective of the rate of change, ICTs transform the way citizens receive information while opening up channels for political discourse—a clear information improvement over broadcast state media (199). Howard concludes *Digital Origins* in Barrington Moore's advice that there is not a singular path to democracy. However, Howard's work concludes that there is a strong trend and causal relationship between technology diffusion and democratic transitions (200). Thus the democratization pathway now is undeniably digital according to Howard, but this may over-emphasize and underestimate existent, alternative political opposition networks that initiated the uprising. Moreover, even after the multiple political upheavals, Egyptian repression continues in the streets and through ICTs because there was never a complete transition out of authoritarianism in Egypt.

ICTs in the Arab Spring

The Egyptian regime responded to the increased public sphere online by blocking access to social media sites like Twitter and Facebook occasionally in the years leading up to the Arab

Spring. This sporadic behavior shows that regimes were worried about ICTs before their massive adoption and that authoritarian states struggled to find a way to choke off democratic thought without appearing too harsh. In other words, unlike China, Egypt failed at networked authoritarianism. In 2008 Tunisia blocked Facebook for a month (Howard 39). In 2011, a protestor in Tunisia lauded Facebook, ""Facebook is pretty much the GPS for this revolution…Without the street there's no revolution, but add Facebook to the street and you get real potential" (Streetbook). Undoubtedly the regimes feared this ease of communication spurred by these platforms and their ability to form bonds outside of one's typical circle of friends—and to engage in discourse with similarly concerned citizens (Howard *Digital Origins*, 39).

Howard considers Wael Ghonim, the Google regional executive, as instrumental to the social networking uprising in Egypt. Ghonim created the "We are all Khaled Said" group on Facebook, which organized a mass amount of people to the streets on January 25th. The virtual group memorialized the blogger beaten to death in the streets of Alexandria in June 2010. In the Iranian Green Movement, the death of a young protesting girl was memorialized to catalyze collective action (Howard *Digital Origins*, 23). This large social network revolutionized the idea of civil organization and provided a means for mass civil disobedience manifested in the public gatherings in Tahrir Square (Howard *Digital Origins*, 22). Similar circumstances emerged from the street vendor, Mohamed Bouazizi, who lit himself on fire (Howard *Digital Origins*, 18). His digital memorialization sparked unrest in Tunisia in December 2010, which shortly spread to Egypt in January 2011.

Cyber-Utopianism and Digital Repression in Egypt Post-Arab Spring

In Tunisia social media networks helped with twenty-percent of the population with accounts, but nearly everyone had a cell phone, again reinforcing digital tools that are not

necessarily the Internet (Howard *Digital Origins*, 19). Similarly, virtually all Egyptians possessed phones, hence SMS messaging established networks for "collective action and a collective goal—to depose their despot" (Howard *Digital Origins*, 19). Uploading real-time images to social networks immobilized security forces' reaction to mass protests. When videos captured police brutality at the protests, YouTube allowed for the "carnage" to be uploaded. This user-driven ability had local, regional, and global ramifications. Castells adds how the Tunisia example instilled hope into the Egyptian protests:

> Tunisia epitomized the hope for change. It showed that it was possible to topple a well-entrenched regime if everybody would come together and fight uncompromisingly, to the end, regardless of the risks. The Internet provided the safe space where networks of outrage and hope connected (81).

The spotlight on Mubarak became brighter and the level of collective action strengthened at all these different levels. Yet, how well-entrenched was a Mubarak regime that did not have a definite plan on how to react to the growing digital unrest? Moreover, the military takeover arguably enhanced the state's ability to filter and control information over the web. According to Reporters Without Borders, the Supreme Council of the Armed Forces (SCAF) that filled the political power vacuum after Mubarak's abdication, practices censorship and intimidation. In military courts, journalists and bloggers were sentenced to years in jail for "insulting the armed forces" (Reporters Without Borders). Protests remerged later in 2011 against the harsh military rule. Again, bloggers were targeted and assaulted, one blogger; Malek Mostafa lost an eye when security forces forcibly dispersed the crowds in Tahrir Square.

Although the Internet may have seemed like a safe space from Castells' point of view in 2011 and 2012, the current regime in Egypt cracks down on ICTs. Again the government warns users of social media, "that they could be arrested for inciting violence through their posts, which were being tracked by the state" (Al-Jazeera). This threatens the civic duty each blogger and

journalist performs when they risk their lives while criticizing the government online in a traceable form. The persistence of this hostile atmosphere towards bloggers and journalists persists despite these uprisings. This reinforces that what occurred after these popular mass movements was not an actual revolution but a symbolic sacrifice of a figurehead.

Western technology companies often enable authoritarian regimes to purchase devices that "restrict the flow of information" (Howard *Digital Origins*, 173). The example of the Arab Spring encourages all authoritarian regimes to stock up on such censorship and surveilling equipment necessary to impede grassroots movements online. When online news stories are trending or "go viral," they signal to the regime a rising challenge to its power. In this sense, monitoring the ICTs helps authoritarian regimes anticipate and react to festering insurrections. In fact, Mubarak was able to attempt to shut down the Internet by asking British-based Vodafone to disconnect Egypt's phone and Internet service and bought surveillance technology from an American company, Narus (Democracy Now). The product called "Deep Packet Inspection" allows the telecommunications companies in Egypt to open up online communications and track dissident behavior and tag their geographic location (Democracy Now). The Iranian Revolutionary Guard stifled its own social insurrection in 2009 after purchasing systems from Nokia Siemens.

The result of this process of building up a vibrant civil society launched a massive protest in Egypt roughly estimated at over 10 million people, over a thousand casualties, and thousands more injured (Howard, 9). In addition, over 12,000 people were arrested before Mubarak's thirty-year regime ended (Howard and Hussain, *Democracy's Fourth Wave*, 9). In the cases of Egypt and Tunisia, both dictators conceded to the public demands. Yet the experiences in Bahrain and Iran were successfully impeded, whereas in Libya and Syria protests and

government reached a political impasse (26). Like Howard says, digital media can promote democratization, but it is by no means the sole causal factor. Demands for justice and government accountability are prominent amidst the organizers of the mass movements, but more generally protesters in Tahrir Square demanded "bread and dignity" (Zurayk and Gough, 107). Thus, Howard resists the media's call to label these social movements as strictly "Twitter or Facebook Revolutions;" rather, "technology tools and the social actors who use them, together, make or suppress political uprising" (31).

Overlooking ICTs

The over-glorification of ICTs blurs the role of existent alternative political oppositions that facilitated the coordination beyond the logistical sharing that ICTs facilitated. The mixing of rival soccer fan groups marks a unity that was rooted in political opposition and amplified by ICTs. The Muslim Brotherhood has been a consistent political alternative despite its subordinate position during Mubarak's dictatorship. "The Ultras, [a group of soccer fan clubs] fought battles, they understood organization, they understood logistics and they understood fighting a street battle with the police…And in that sense they played a very key role in breaking the barrier of fear" (Pollock). The ICTs democratizing effects can be channeled to bring together separate groups. But, beyond the act of coordination, ICTs do little to stem military repression. In fact, the manipulation of ICTs leads to the detainment of bloggers (Pollock).

The grassroots mobilization on the Web was initially sparked by the anonymity on online networks. Furthermore, online activists reveled in these digital shadows by posting information critical of the government without their names attached (Howard and Hussain, 38). The platform of the Internet and information technologies added a weapon to the grassroots movement in Egypt. Mubarak fumbled the problem; when he shut down the Internet, he only disabled

broadband connections, not satellite connections (Howard and Hussain, 41). Egypt's example may be a case of an ineffective, antiquated regime flailing to become sophisticated digital repressors. If this hypothesis holds true, then the future for democratization via technology diffusion in other authoritarian regimes may be doomed. Moreover, Egypt is not a transferable example because military rule continues repression despite the widespread use of ICTs. Despite technological diffusion that prompted the initial uprisings in 2011 digital civil society has been effectively constrained by an authoritarian government equipped with sophisticated censorship, surveillance tools and classic repression methods.

Continued Military Repression in a Tightly Controlled ICT State

In the aftermath of Mubarak's resignation in late 2011, life in Egypt was the same politically and even more chaotic. Howard claims that technologies and actors who use them can "make or suppress political uprising" (37). In light of the political fragmentation of Egyptian society between secular democrats and the Islamic Brotherhood and persistence of repressive military rule, the situation appears more alarmingly like the latter than the former. Despite the process of parliamentary elections that consolidated party formation and continued protest against military rule, created an atmosphere of, "the bizarre feeling of status quo minus the stability" (Middle East in Focus, 357). Violent clashes with military personnel did not end once Mubarak resigned; they continue to protect their power with repression and ICT manipulation. Additionally, the mass mobilization of various groups do not share the same agenda, and no amount of ICTs could change this inherent political problem.

In the aftermath of the Mubarak regime, the government increased content filtering according the Internet Monitor, a tool from the Berkman Center in Harvard that analyses online content and activity globally. Furthermore, the regime continues to temporarily block sites like

Facebook, Twitter, and Bambuser, while also physically arresting bloggers and human rights activists. Aside from digital repression, military rule in Egypt has resulted in dissent repression via prolonged detainment, excessive mass prison sentences, and murder. After the Morsi removal in July 2013 the Egyptian military reinforced its rule by "methodically" firing live ammunition in crowds of demonstrators opposed to the Morsi overthrow In August 2014, Human Rights Watch released its findings:

> The systematic and widespread killing of at least 1,150 demonstrators by Egyptian security forces in July and August 2013 probably amounts to crimes against humanity, Human Rights Watch said today in a report based on a year-long investigation. In the August 14 dispersal of the Rab'a al-Adawiya sit-in alone, security forces, following a plan that envisioned several thousand deaths, killed a minimum of 817 people and more likely at least 1,000.

When compared against the harsh realities of political control, ICTs shaken regime power and cause it to repress brutally to negate any ICT liberalization. Largely peaceful protests at Rab'a al-Adawiya Square for over a month violently ended on August 14 with mass casualties. Kenneth Roth, the executive director of Human Rights Watch says:

> "In Rab'a Square, Egyptian security forces carried out one of the world's largest killings of demonstrators in a single day in recent history…This wasn't merely a case of excessive force or poor training. It was a violent crackdown planned at the highest levels of the Egyptian government. Many of the same officials are still in power in Egypt, and have a lot to answer for."

Roth's comments make it clear to what lengthens the military regime will go to reinforce its power through violence. Egypt in 2015 is more chaotic than 2011 thanks to ICTs and the threat of liberalization that solidifies regime repression.

Conclusion: Repression and ICTs

Castells insists personal networks established online thrive off of people seeing other people organize and protest. These actions are linked to their online social persona that bears their actual name. Hence Castells writes, "The key to the success of an SNS [social networking

sites] is not anonymity, but on the contrary, self-presentation of a real person connecting to real persons" (232). However, the crackdown on said brave bloggers and social networkers presents a challenge for a persistent, viable digital civil society. The continuous political unrest blurs any consensus once built by disposing of Mubarak. Furthermore, the overthrowing of the democratically elected Morsi increases instability and the repressive apparatus of the military encourages fear and complicity online.

Despite the Egyptians' proclivity to mobilize in mass numbers quickly, this ability is minimized when its general consensus is reversed several months later in a cyclical basis. The unrest of the Egyptian political system is the perpetual miscommunication between leadership and the people. No amount of tweeting or blogging can circumvent this core governmental problem. This issue manifests itself in the arduous task of drafting a constitution that strikes a balance between Islamic beliefs and constitutional law. This is not to say that the ousting of Mubarak, and latter Morsi, was for nothing. Revolution is a bloody mess that takes time to build consensus; according to Robert Bowker in 2013, "a populist, chaotic political period lies ahead, with elements of xenophobia even closer to the surface of political discourse than during the Mubarak era" (591). The Arab Spring proves that ICT are a beneficial tool to the mass citizenry when bringing down an authoritarian regime that does not adequately contain the liberalizing effects of ICTs. The most significant lesson from the Egyptian case is the futility of ICTs as a political unifier or apparatus for complete political revolution. The efficacy of said tools has not been productive in building peaceful consensus and restoring order as evident in Egypt. ICTs cannot stop military repression, but have actually proven to catalyze it. Again, this reflects the idea that ICTs are tools, not a substitution for political democratization. Thus, the military protects it power via a crackdown on the Web and in the streets that effectively eviscerates the

little political power ICTs once possessed.

Chapter 5, Part I: U.S. Digital Grassroots Movements

Introduction

The Internet in the United States has undergone massive changes from its inception as a noncommercial project to its evolution into commercial use. The technological development from email to social media revolutionized the way we communicate and interact with others. In 2012, efforts to thwart censorship legislation were successful, while later, in 2013, the Edward Snowden revelations uncovered Orwellian surveillance tactics secretly codified by a secret court. Two defining events in the past few years have changed the landscape of what political power can be extracted from the Web and ICTs. First, the Occupy Movement boasted the power of the Web to facilitate social mobilization that enacted simultaneous nationwide protest encampments in the early Fall 2011. The Occupy movement practiced non-violent civil disobedience akin to the memories of peaceful protestors like Gandhi and Martin Luther King Jr., by utilizing more inclusive digital technology to activate similar-minded organizations. Yet, the NSA revelations in spring 2013 by Snowden pushed back against this liberalizing perception of the Web. The vast NSA surveillance dragnet counteracted and even pushed the balance of power of the Web from the people unequivocally to the side of the state, thus severely delegitimizing the cyber-utopian perspective of ICTs. The very technologies boasted as democratizing by the U.S. were actually being used to track and surveil the electronic communications of subjects and citizens both abroad and domestically. This chapter seeks to unite how these two narratives converge and why surveillance is damning for a liberal democracy and its people's ability to freely counteract the status quo.

Occupy and ICTs

Camped out in Zuccotti Park, Americans from all walks of life protested the unequal structure of American society in the aftermath of the Great Recession for sixty days. The Occupy movement platform emphasized the ninety-nine percent, composed of the masses, versus the one percent, which epitomized the ultra wealthy. The platform reflected the sharp economic divide in the nation; the top one percent held forty percent of the nation's wealth (Fault Lines documentary). Although they lacked a rigid list of demands, the Occupy movement—a people's movement— was a political protest that refused to legitimize the current political structure that unequally favored the elite (Fault Lines documentary). Outraged by the bank bailouts and the effects of the recession, "Occupy" acted outside of the levers of government. Instead the movement occupied public space to reclaim the commons by stressing a radical democracy that adheres to the people, not the power holders. Castells stresses the symbolism of seizing spaces of places, "from where they could challenge, by their presence and their messages, the financial spaces of flows from where global powers dominate human life" (178).

The Occupy movement used the crowdsourcing abilities of Facebook and Twitter, and other non-proprietary social networking sites, to mobilize a mass movement. Like Egyptians that flocked to Tahrir Square, New Yorkers and Americans used ICTs to coordinate times to occupy parks and other public spaces for weeks and months. The movement described itself as an inclusive, direct democracy that aimed to strike in the midst of atmosphere of political discontent (Pew Research figures). The movement went viral and swept across the states with other Occupy camps in Boston and Oakland. The original idea of Occupy came from a Canadian digital magazine, *Ad Busters*, which circulated amongst American organizational groups in the summer of 2011. Eventually, the date to occupy Wall Street was set for September 17th (Adbusters).

Here, digital communications were helpful in linking similarly-minded groups, not spontaneously creating new ones, but strengthening bonds to form a larger movement.

The Occupy movement did make use of ICTs to facilitate typical organization methods and coordination efforts. The magazine offered digital ways to solve logistical problems e.g., "techies" built an open source website that arranged transportation for protestors to New York (*Ad Busters*). Organization for the Occupy movement occurred online initially, which allowed people to meet up for real-life events. *Ad Busters* adopted the hashtag #occupywallstreet on June 9, 2011, to begin a collective space on the web to spread awareness of the movement, both logistical and informative (Castells, 171). The front page on *Ad Busters* evokes the Tahrir Square spirit by posting different slogans like, "Stop the Monied Corruption at the Heart of our Democracy," which spread across social media networking sites (*Ad Busters*). The inclusive nature of the Occupy movement enhanced the already established digital relationship between activists and their organizations.

Micah White, an organizer for the Occupy movement, was inspired by the Internet and ICTs widely as tools to coordinate global action (Esquire). White cites the internationally coordinated February 15, 2003, protest against the impending Iraq war as a global movement impossible before the Internet age. Despite his optimism for global coordinated action, White believes protest will not enact immediate political change, but would help raise the collective consciousness of the public. He favors a global coordinated shift in protest paradigm that mobilizes social movements to change their "behaviors and depattern themselves, to actually collectively get facts to tackle global challenges" (sic)(Esquire). Thus, White's outlook sides more with cyber-realists, value the Internet as a tool, but realize policy enacts political change more so than technology, or technologically spurred protests. The ability to set the date to

occupy Zuccotti Park online went viral, allowing many more people to see it than possible in a pre-digital era. The Occupy movement resembles the organization process of the 2011 Egyptian uprisings in which ICTs acted as an excellent tool to direct individuals outrage into a large, public protest. However, the repressive state apparatus minimized the Egyptian ICTs, which leads to the question: how effective would the grassroots ICTs be in a democratic context in the U.S.?

Early Internet Ethos

The organizers of the Occupy movement and early adopters and creators of the Internet share a suspicion of government power. This early Internet culture idealizes the Internet as a great equalizer that empowers people rather than the government. John Perry Barlow's "Declaration of the Independence of Cyberspace," uses language that depicts the Internet as a utopian realm in which the people rule, not the state:

> We are creating a world where anyone, anywhere may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity. Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are based on matter, There is no matter here. You [United States] are trying to ward off the virus of liberty by erecting guard posts at the frontiers of Cyberspace… In our world, whatever the human mind may create can be reproduced and distributed infinitely at no cost. The global conveyance of thought no longer requires your factories to accomplish.

This grandiose rhetoric mirrors the Occupy movement's refusal to operate within the levers of government to vocalize their demands. Instead, they assert these demands on the street and over the Web. The Internet's utopian beginnings and desire for a good place that is no place—outside of jurisdiction of governments—is the origin of digital resistance to the commercialization and government ownership of the Web.

The architecture of the Internet initially fueled the cyber-utopian movement. The Internet's design is "a loose arrangement of connected but autonomous networks of devices" (Ryan, 31). The open and decentralized essence of the Web resembles the cyber-libertarian ideal

of an un-regulated space. Moreover the actual creation of the Net by the early pioneers emphasizes an open collaborative effort to build a "technical, open design" (Ryan citing Crocker, 32). This group of graduate students poised to build developing working protocols to connect networks stressed a "humble and inclusive posture" epitomized by the mantra, "rough consensus and running code… to agree on proposed standards" (Ryan, 33). The efforts of the early Internet pioneers culminated in developing the end-to-end principle that "moved control over the operation of the network from the connecting infrastructure to the actual devices participating in the network themselves" (Ryan, 38). Zittrain agrees that this resulted in an Internet, "in which no one in particular owned and that anyone could join" (30).

Similarly, in Zuccotti Park, organizers practiced non-hierarchical, horizontal organizational structures to make decisions, including how long to stay, how to get food, and how to counteract gender biases within the group (Fault Lines documentary). Occupy sought to build a rough consensus amongst people from all ethnic socio-economic/political backgrounds to aggregate the ninety-percent for a "running," or working government for the people. Like the Internet, Occupy practiced a decentralized organization structure to practice non-violent civil disobedience. Ironically, the Occupy movement harnessed the liberalizing effects of ICTs to reach the widest audience for their inclusive ideas.

The Permanency of Digital Content

The current civil society in the United States thrives because of its interconnectedness. Facebook and Twitter are credited for easy spread-the-word campaigns. Other ICTs, like live streaming, gained prominence as a transparent tool that could send live video feeds to people across the country and world. The Occupy movement credits technology as a means of coordination, as a way of learning from each other, and the ability to record everything (Fault

Lines). Livestreams and videos uploaded to YouTube "give people a window into the movement," says Josh Boss, an information technology worker for Occupy (Fault Lines documentary). Live feeds allowed Occupy to make its own coverage, while mainstream media either did not cover some aspects of the movement or refused to cover it entirely. Yet, what forced media to start covering the protests was when cops used repressive tactics like pepper spray, which sparked a larger public outcry. From the Occupy position, the live feeds allow for nothing to be hidden (Fault Lines documentary).

Despite these technologies, police in Oakland, University of California-Davis and New York all used force to disband encampments. In the early morning of October 25th, 2011, police surrounded the Occupy encampment under the cloak of darkness and forcibly removed protestors (Castells, 163). Police relied on tear gas and flash grenades to vacate the premise. Over a hundred protestors were arrested. Most importantly, a video caught the injury of an ex-Iraq war veteran, Scott Olson, which put into public focus police brutality. Nevertheless, evictions continued across the nation, which were covered by mainstream media. A video went viral when a police officer pepper sprayed Occupy students at point blank range, emphasizing Castells' point that movements are viral since captured abuse inspires mobilization (224). On November 15th, the birthplace of the Occupy movement in Zuccotti Park was similarly forcibly removed with the same pepper spray tactics in the middle of the night.

Despite police repression and plentiful arrests of peaceful occupiers, Castells argues that the ability of the Internet to continue the protest conversation in a cyber setting is a unique attribute of digitally infused protest: "The Occupy Wall Street movement is a hybrid networked movement that links cyberspace and urban space in multiple forms of communication" (177). ICTs enable many different ways to tell the story of protests by uploading pictures and videos,

allowing viewers and history to judge the events as they appeared through these lenses (Castells, 178). The example of the UC-Davis incident may force gradual changes to police treatment of peaceful protestors. Although the power of these videos expose abuse and promote transparency, they are indicative of the minimized capacity of ICTs in complicated political contexts. The permanence of content online does little to facilitate change after the protests occur**.**

Now, approaching the four-year anniversary of the first encampments, the Occupy movement has been muted by competing concerns within the U.S., namely police brutality and state surveillance, spurred by the Snowden revelations. Although the Occupy movement lost salience in its own name, the movement exists digitally on many autonomous blogs—like www.occupytogether.org and occupywallst.org—by sharing links to spread Occupy news. What the Occupy movement accomplished was a raising of consciousness that was primarily felt in the spectacle of literally occupying public spaces. Yet, the political power of the state physically repressed and shut down the movement. Without a public presence, the Occupy movement disappeared from the public eye, despite its sophisticated use of technology. Yet the movement achieved considerable success, it imprinted on the American consciousness an alternative, although somewhat vague, to the status quo. Technology undoubtedly spurred the movement across the nation, reaching far more supporters across a wide geographic area than previously possible in a pre-digital era. In terms of political power, the Occupy movement successfully organized mass demonstrations, but to no political avail. Yet, the movement, if only temporarily, harnessed the political power of the multitude, despite its eventual collapse.

Anonymous' ICT Power

One grassroots movement, before and after Occupy, that uses the Web as a political tool with success is the hacktivist group Anonymous. Born from online communities interested in

sharing jokes and memes, Anonymous emerged initially as an immature, apolitical community that evolved into a digital counterforce to unjust practices that wields considerable cyber and political power. The idea of Anonymous—a band of hackers without any structure or leaders—, matured from Internet jokes to political activism while first battling the Church of Scientology in 2009. An embarrassing video of Tom Cruise excitedly talking about Scientology leaked onto the Internet and Scientology promptly forced YouTube to take it down. In response to the censorship, Gabriella Coleman describes a "call-to-arms" amongst 4chan.org users to employ cyber methods to "hack" the scientology website and "take it down" (55). Users on 4chan bounded together to use a simple form of cyber warfare—distributed-denial-of-service (DDoS) attacks—, that generates thousands of requests for access to a website that eventually overwhelm the site, causing it to crash and become inaccessible. An Anon (a member of Anonymous) wrote of Anonymous' strategy against Scientology: "Keep in mind this is a war of attrition. WE cannot bankrupt Scientology directly—this about getting media attention, informing the pubic, wearing down their members, pissing off their IT/phone services, counter-brainwashing their potential recruits, and for lulz[hacker jargon for laughs]" (sic) (63). After several years of battling Scientology, the public perception Scientology group became more negative and membership dwindled; a success partly attributed to Anonymous' publically waged battle that captured the attention of the mainstream media. The key to Anonymous' strategy is its decentralized organization composed of many different networks (Coleman, 75). Thus the digital civil disobedience era began by aggregating like-minded hackers to contribute to a just cause in a remarkably decentralized manner that is difficult to trace.

Beyond Scientology, Anonymous targets companies, groups, and individuals, anyone that threatens freedom of speech on the Internet and other liberal ideals like freedom generally.

Anonymous is a grassroots movement like Occupy, except that it thrives behind computer screens with its digital arsenal of hacking techniques and ability to generate digital outcries that transform into real protests on streets. Luke Goode writes: “The ethos of Anonymous is technophilic and digital technology is heralded not only as a way of life for group members but also as a driving force for reshaping society” (Goode, 75). In other words, Anonymous, although rooted in an online community, became a political force that sets an agenda, which promotes social justice and freedom from electronic surveillance and Web censorship (Goode, 83). For example, Anonymous recently identified thousands of Islamic State twitter handles and submitted them to be banned by Twitter.

Scholars find Anonymous difficult to label—some say it’s a cyber-libertarian organization while others describe it as a strain of anarchistic, “trickster politics”. What is clear, however, is that Anonymous is a product of the Internet age. Its organization is decentralized and composed of all different, anonymous people who share computer skills and an affinity for activism. They view themselves as a sort of vigilante group that counters corruption, whether it is towards corporate entities like PayPal, or states, like ISIS. Goode doubts Anonymous’ ability to engage with policy reform since it is a subculture group with little appetite for mainstream politics. Yet I argue that their periphery status from policymaking is what makes Anonymous valuable for the future of a digital democracy. Hacktivism ensures anonymity and collectivity against abuses of power; however, its proclaimed inclusivity is not as tangible or evident as Occupy’s ability to populate parks (Goode, 84). Yet, when geared towards liberal causes and protecting the integrity and ethos of the Internet, Anonymous elicits a sort of democratizing “people power” from their computer skills. If there is a real example of cyber-libertarianism, Anonymous is the best fit, yet it is hardly a widespread movement, although it is inclusive.

Transparency

The reproducibility of electronically stored information enables users to copy and share information cheaply and quickly. Now in the digital era often the "least trusted person" in an organization has access to many troves of documents and only requires a USB drive to copy the information and leak it. The wholesale disclosure of the top-secret documents as experienced in Wikileaks exposes state abuse—like the covering up of the US airstrike in the 2007 that mistakenly and provokingly killed *Reuters* news staff and ten Iraqis. Wikileaks, whose motto is "we open governments," posted a video of the incident, entitled "Collateral Murder," that caused public uproar (Sifry, 142). The ability to upload information, which anyone can access, is radically democratizing access to information. This information puts pressure on governments to answer to potentially hypocritical standards.

Piling information on the Web may be transparent, but it does not immediately enact political change (Open Government). Thus, WikiLeaks is the digital age equivalent of the Pentagon papers released by Daniel Ellsberg, except it reaches a wider audience thanks to using the Web as a tool. What is important about this new age of transparency is the content of these leaks. More specifically, Snowden's leaks provide classified information about U.S. intelligence agencies' elaborate surveillance systems. The freedom of this information released through journalist intermediaries challenges the American national security establishment with difficult questions about the constitutionality of state surveillance, much like Wikileaks questioned American rules of engagement in wars and contradictions in diplomatic cables (Sifry, 140). With this in mind, the cumulative effect of transparency may foment political unrest and protest to achieve the goal of transparency: "to achieve a more just society," according to its founder, Julian Assange (Pieterse, 1918). Thus, "WikiLeaks exposes the tensions between democratic and

hegemonic transparency" (Pieterse, 1917). Although the NSA revelations were disclosed almost two years ago, the state surveillance systems are still in action and have not been restrained legislatively. Yet with the sun-setting on Section 215 of the Patriot Act on June 1, 2015, many activists, political organizations, and journalists seek to sway public opinion to pressure Congress to enact legislation that reforms these systems that are questionably unconstitutional, thanks to transparency.

Chapter 5, Part II

Digital Grassroots Power v. State Power

The power of the Occupy movement and even Anonymous is in the multitude, whereas, the power of the state in this digital world is in the collection of data (Schneier, March 25, 2015). Like in Egypt, these ICTs themselves did not invoke the uprisings, but they did catalyze an already-formed group of activists and help coordinate protests. More importantly, the lasting impact of digital technologies that capture police repression would ideally make governments more accountable. In many ways, the power these grassroots movements gain from technological progress is indefensible against, and not on the same level, as the progress made by omnipresent, state electronic surveillance.

State Surveillance

In May 2013, Edward Snowden handed over top-secret information about the United States' intelligence services, primarily focused on the clandestine operations of the National Security Agency (NSA). Working as a contractor for Booz Hamilton, Snowden had access to information about how the government utilizes the Internet as a tool for collecting information and staving off international and domestic threats. The high-degree of control over ICT data collection exerted by the intelligence agencies and their contractors weakens the alleged liberalizing effects of these tools. In collusion with large technology companies, and sometimes without their knowledge, the NSA tracks and collects virtually all electronic communications in the world. The revelations made by Snowden have reverberated around the globe and called into question the constitutionality of the Patriot Act. First, I will outline clandestine NSA programs that collect and store the data produced by citizens' devices and were guided by the motto to

"collect it all,"—"all" meaning the entirety of electronic communications both domestic and global (Greenwald, 95).

The Programs

Before the NSA revelations, leaders of the agency often dismissed its ability to collect telephone calls and emails—it only had such a capability for targeted foreigners, they alleged. However, the program, "BOUNDLESS INFORMANT," is a data log of all the telephone calls and emails collected every day around the globe "with mathematical exactitude" (Greenwald, 30). Greenwald emphasizes that the existence of this program proves that former NSA Chief Keith Alexander had lied to Congress when asked whether he had a quantifiable estimation of data collected by these programs (92).

The program PRISM enabled large-scale data collection directly from the servers of the world's nine largest Internet companies, including: Google, Yahoo!, Microsoft, Apple, AOL, Facebook, Skype, YouTube, and PalTalk (Greenwald, 94 and 108). In lieu of petitioning the Foreign Intelligence Surveillance Act (FISA) court for each request of information, PRISM empowered NSA agents to scour through companies' information without any interaction, or informing a company's staff (Greenwald, 108). In 2006, Lawrence Lessig explained how electronic communications are more susceptible to monitoring and searching because of their "traceability" and intangibility (47). More concerning, the transition into the digital age improves monitoring capabilities without increasing the burden on the individual search (Lessig, 23). A user cannot tell if an NSA agent hacked into his or her email account—there is simply no trace for the common citizen to identify. Combined with the NSA's alliance with Internet service providers (ISPs) and hardware companies like Apple, users' data is vulnerable form the moment a new phone is taken out of the box. Documents disclosed by Snowden also show the existence

of a program, SIGNIT, which allows intelligence agencies to lobby technology companies to build certain vulnerabilities into their design to make data collection easier (*Guardian* files). In addition to the unprecedented level of access to users' data, its digital form is conducive to collection in a highly efficient manner that is easy to trace what a user does on the Web (Lessig, 80). Again, these collections are all encompassing and not subject to typical "probable cause" warrants to justify each surveillance of communications. Thus, the NSA program is dubbed a mass surveillance system.

When thinking of what the NSA actually collects, it is best to separate the data into two categories: content and metadata. Programs like PRISM capture both forms of data. It captures the text of emails and other electronic communications. Metadata is an especially useful form of data that seems less intrusive since, it denotes mathematical information of a person's whereabouts via GPS tracking, the length of a phone call, patterns of phone calls, and the geographic location of each side of the call. This data uncovers patterns and can help form a narrative, which may not be true, based on the information provided. Metadata of GPS location which comes standard in today's iPhone's operating system, unless disabled, provides information of where the user is located all times, and for how long on a map. Schneier asserts why GPS data is useful to the power of a state. In the NSA, databases named HAPPYFOOT and FASCIA, are used to "track people's movement, identify people who associate with people of interests, and target drone strikes" (Schenier, 3). For instance, my phone knows when I leave the house on which days and where I go. Proponents of the metadata surveillance argue that the name of the user is not disclosed, thus alleviating its intrusiveness. The identity of users who are targeted by these intangible programs is knowledge known only by law enforcement and federal agents, they allege. In response, the indiscriminate nature of metadata allows for algorithms to

assert that every citizen is a possible threat, without giving any reason to suspect a citizen, or all citizens, of wrongdoing. The ability to tap into this information and maintain this information when there is no probable cause for every individual citizen is the epitome of a mass surveillance system gone astray and problematic to the core values of a democracy.

XKEYSCORE is the agency's self-described "widest-reaching" system for collecting electronic data (Greenwald, 153). Using a user's email address, XKEYSCORE captures nearly everything a typical user does on the Internet from the text of email, to browser history and Google searches (Greenwald, 157). It is most effective when used in the context of social networking sites like Facebook, which grants the agency "insight in the personal lives of targets" (Greenwald, 158). BLARNEY is a specific program that specializes in monitoring Facebook data and activities (Greenwald, 160). The NSA also developed a program to collect information previously thought impossible, whilst mid-flight on a plane, enforcing the agency's commitment to collecting all data (Greenwald, 95).

The Vague Legality of Mass Surveillance

The rationale for legalizing invasive means to electronically track communications lies in the enactment of the Patriot Act in the weeks following the September 11th attacks. The Patriot Act seeks to unearth more information in order to thwart more clandestine attacks. However, the problem was not a lack of abundant information; to the contrary, it was the insufficient sharing of information between agency bureaus. The 9/11 Commission Report blamed the attack on the multiple intelligence agencies' "structural barriers" that contributed to an overall inability to connect the dots, despite possessing information that could have prevented the attacks (408). Regardless, in a time of crisis and panic, Section 215, amendments 501, 502, and 503, of the Patriot Act amended the Foreign Intelligence Surveillance Act of 1978 to enable the mass

collection of telecommunications of U.S. citizens (Section 215 text). The first piece of information revealed by Greenwald via Snowden to the public was the memo that forced Verizon to allow NSA access to their communication logs of all its users, by way of Section 215. Reauthorization of Section 215 has paved way for mass surveillance by rephrasing the text to include users' data, both telecommunications and Internet data.

How Data can be Controlled by Design

Lawrence Lessig bluntly stated that in this digital era, "code is law" (Lessig citing Joel Reidenberg, 5). In the preface to his book *Code 2.0*, Lessig reflects how the vision of the cyberspace was egalitarian and democratic. The as unregulated is no longer attainable, despite the optimistic fervor of early cyber-libertarian Internet pioneers and designers. While the Internet was being invented thanks to government-funded research, early pioneer programmers sought to design a decentralized network that was non-proprietary. Yet the e-commerce bubble that lasted from the mid-90s to the mid-00s revolutionized businesses and commercialized the Internet thus eviscerating the cyber-libertarian potential of the Internet. Lessig approaches the future of the Internet by posing it as a choice between liberty and control. However, in order avoid the devolution of the Internet into a tool of control, the early ethos of the Internet movement needs to be resuscitated. Lessig seeks to maintain the democratizing effects of the Internet like open and free source, decentralization, anonymity, creative commons, and free transfer of information that thrive from an open Internet, rather than a closed network.

What fueled the optimism for cyberspace as an egalitarian, democratic haven was its minimalist design that intentionally reflected a political decision to disable control (Lessig, 44). The end-to-end principle is the core principle of the Internet's architecture that allows "a wide range over very different functions" (44). Hence the design for the Internet was publically

available and shared for innovative and transparent purposes (Lessig, 45). In order to accomplish this design, it places trust in the other end to competently maintain their end of the network (Zittrain, 31). Instead of opting for a specific use of a network that was not adaptable to other innovative uses, the simple architecture of the Internet facilitated innovation by being open source, meaning it allowed users to build on each other's work to make better code and more user-friendly program or software. For example, Mozilla Firefox is an example of an open-source browser built by thousands of different coders all driven to the same goal– to create a non-proprietary alternative to proprietary, commercial browsers like Safari and Google Chrome. The insistence on non-proprietary code is consistent with the ethos of the first programmers who envisioned and created the Internet as a decentralized, non-commercial haven (Code 1.0 Lessig, 39).

Yet Lessig recognizes that cyberspace—the space in which a user engages with others on the Internet—can be regulated by its architecture, or design (Lessig, 32). Similarly, Jonathan Zittrain forebodingly addressed the vulnerabilities in the Internet's architectural design in his book *The Future of the Internet and How to Stop It*. Lessig would argue today's Internet is a closed proprietary network that creates an architecture that facilitates control (37). Thus, Lessig warns, "cyberspace, left to itself, will not fulfill the promise of freedom. Left to itself, cyberspace will become a perfect tool of control" (Lessig, 4). Lessig explains that the trajectory towards cyberspace being regulated is driven by "purely pragmatic commercial ends…not the product of some *1984*-inspired conspiracy (38). Although that may be true—that the Internet's promising egalitarianism is sufficiently tarnished by the commercialization of the web, Lessig refrains from describing this shift as nefarious. But now, in the context of intelligence agencies exploiting the ICTs as means of control, Lessig's work is eerily foreboding. The manipulation of the Internet's

original architecture creates a system of near perfect control, which not only constrains the aspirations of the early programmer movement, but also impacts the political efficacy ICT users.

Excessive State Control

In the light of Snowden's revelations, Lessig's cautionary tale bore fruit: the NSA had manipulated the architecture of the Web as well as corrupted the privacy agreements of technology firms and Internet Service Providers (ISPs). Lessig writes how the government applies pressure to companies to "build their systems to collect and preserve a kind of data that only aids the government" (Lessig, 65). PRISM is the program that not only directs how companies log their data, but also requires an NSA access point. In the scope of this thesis it is important to address this concept of collecting one's information stored for example on Gmail when Google allows NSA backdoor access to its users' communications. "Data collection is the dominant activity of commercial websites" according to Lessig (219). However, this statement becomes complicated once it is realized that the government taps into the data collection of technology companies and fiber optic cables. The same can be said for the iPhone and other major Internet companies that collude with the government's mass surveillance system.

Lessig and Zittrain illustrate a creation story of the Internet as designed to be open and emphasize its motive "had little concern for controlling the network or its users' behavior" (Zittrain, 28). This vision starkly contrasts with the current state of control of the Internet. Zittrain notes how the commercialization of the Internet created new media kings like Facebook and Google, which filled the vacuum of traditional old media and monetized the Web. The values of free speech and instantaneous communication that pervaded the early Web movement were compromised for control. The NSA's operations manipulate the Internet's architecture and attempt to centralize all its communications in a vast decentralized network to fulfill its

organizational motto—"collect it all," since digital information is traceable. Thus, the NSA's ability to collect information relies on who controls the endpoints of users' information—ISPs and technology companies, which are under the burden of Section 215 to provide all data to the NSA.

Data is Control

The intense prioritization of capturing data reveals the power of the Internet as a data pool of users conducive to digital extraction. More importantly, the NSA's focus on electronic communications suggests its concern for the political efficacy the communication revolution brings with the Internet. Hence, these government agencies seek to collect all electronic transmissions in order to control any perceived threats, no matter how hypocritical such behavior is in a democracy. Political activity in and of itself is suspicious for instance, the NSA surveilled an anti-war march in Akron, Ohio in 2006 (Greenwald, 185). Additionally, mass surveillance has tracked domestic environmental groups as well (Lessig, 210).

To corroborate this threatening feeling, Barton Gellman and Julie Tate found that "ordinary Internet users, American and non-American alike, far outnumber legally targeted foreigners in the communications intercepted by the National Security Agency" (Coleman, 379). In other words, these dragnet systems are justified by a threat from abroad, but are actually used on the general American public. According to Castells, he proclaims,

> Mass self-communication provides the technological platform for the construction of the autonomy of the social actor, be it individual or collective, vis-à-vis the institutions of society. This is why governments are afraid of the Internet, and this is why corporations have a love-hate relationship with it and are trying to extract profits while limiting its potential for freedom (7).

Perhaps governments were once afraid of the Internet, but after Snowden's revelations it is clear—government agencies thrive off data collected legally and illegally via digital tools that make mass surveillance feasible. As a result, the online social networks that take place in the

"free space of the Internet" are susceptible to the fear of being overheard by government agencies. Thus, the movement from outrage to hope is detoured back to fear by state repression in the streets by vacating Occupy camps and online by intimidating users by evoking a big brother figure that equates dissent with wrongdoing.

Lastly, Castells emphasizes the autonomy of the Internet, as though the Web's nature is innately decentralized, allowing for "mobilizing, organizing, deliberating, coordinating and deciding," as well as operating a leaderless movements (as evident in Anonymous) (Castells, 229). Although that may have been true in the early ethos of the Internet movement that created the Internet from "the culture of freedom," today's Internet is compromised by the state's surveillance powers. Again, like Lessig, Bruce Schneier states that the nature of the Internet today is highly centralized and thus conducive to collection. However, Castells argues that social networking sites (SNS) enable the self-presentation of a real person connecting to real persons that enables the transition from fear to hope and hope to political change (Castells, 231). This statement has been proven wrong in states without a democratic tradition like Egypt and China, in which identified users of blogs or videos have been imprisoned and/or killed.

The "Nothing-to-Hide" Fallacy

In the wake of 9/11, government officials often argue that encroaching on civil liberties is the price to pay for safety. Proponents of mass surveillance rely on the mantra that, "If you're not doing anything wrong, *you have nothing to hide*". However, once the government defines what is "wrong," there is a slippery slope for what constitutes wrongdoing. Labeling thoughts or actions as "wrong" simply because they are contrary to the status quo is antithetical to the integrity of a liberal democracy committed to free speech and liberty. When placed in the context of the terrorist threat shortly after 9/11, this argument becomes more tricky, but not necessarily defunct.

Proponents quip, “do you object to TSA searches, simply because they make sure you do have nothing to hide?” In reply, a TSA search is directly tied to a favorable end—to freely travel. It is expected that security measures are enforced prior to boarding a flight as a one-time recurring event. The same is not to be said with the constant search and seizure of all electronic communications. This is not to say that all surveillance is intruding on one’s civil liberties, but massive surveillance without warrants or probable cause clearly violates all citizens’ civil liberties.

But, why should I care, if I am kept safe, is often the reply to concerns over mass surveillance. First, submitting to this state practice is voluntarily diluting one’s constitutional rights, most specifically, one’s Fourth Amendment right to be free from unreasonable search and seizures. By signing off this right without any notice of expiration, it no longer exists and citizens individually and as a whole lose some of their collective political power and right to privacy against a tyrannical government. In the Western perspective, from the Victorian era to the present day, privacy as a concept has evolved immensely into three categories: solitude, secrecy, and anonymity (Miller, 114). The segmentation of homes into rooms separated people and established solitude—the ability to be alone (Miller, 113). In addition to solitude, the concept of privacy emphasizes secrecy or the control of a certain, and sometimes, sensitive information that the world can know about oneself. Privacy tends to be an admission of guilt in today’s society; however, users’ actions often contradict their “nothing-to-hide” rationale. Glenn Greenwald asks—then what prompts users to use passwords on their email and social media accounts? Greenwald reasons that if users truly had nothing to hide, they would not practice privacy controls. Hence, privacy is not nefarious, but relational like (Greenwald citing Gellman). The conversation you have with your friends is not always the same one you want your parents

to hear, and vice versa. Finally, the right to privacy resonates with the right to anonymity or a protection from unwanted scrutiny (Miller, 2011,). On the surface, the Internet seemed to be compatible and protective of these three attributes of solitude, secrecy, and anonymity; however, the traceability and reproducibility of information is instantaneous and cheap. Moreover, the information shared on the Web willingly, like social media, along with information stored or communicated on the Web, under the presumption of privacy, are all equally susceptible to mass surveillance.

Undoubtedly the Constitution faces interpretational challenges in the digital era. The dragnet collection of all citizens' electronic communications indiscriminately is constitutionally unsound. A dragnet means all data is collected, sorted, and stored. The reauthorization of Section 215 makes it clear that "data" are included as tangible things susceptible to this dragnet. Again, the fact that this searching is indiscriminate is more troubling than individualized targeting, because every citizen is then suspicious of illegal activity. Everyone is a suspect, since the few (the NSA) watch (track) the many (the world). This sort of blanket targeting encourages a compliant mode of thinking throughout the citizenry.

State Surveillance as a Panopticon

The idea of the panopticon can be traced back to a prison design theorized by Jeremy Bentham in the eighteenth century (Lyon, 655). The panopticon prison layout placed a guard tower in the middle of a circular prison, ensuring a three-hundred-sixty degree view. The guard tower could see into all of the inmates' cells, but the prisoners could not tell if the guards were actively watching them. This psychological experiment sought to instill a fear of being watched to produce a more compliant prisoner who was more apt to engage in correct behavior since he or she was possibly being watched. The design creates an illusion of an omnipresent force and

was installed as an alternative to traditional prison layouts in which it was difficult to maintain order and prisoner compliance. Yet the idea of the panopticon is most widely known by Michel Foucault's treatment of the panopticon in the context of institutional surveillance (Greenwald, 176). Now the idea of a panopticon is possible with the advent of traceable electronic data. Whoever carries a phone thus carries a personal GPS locator.

The NSA's deluge of surveillance programs creates a panopticon in the everyday lives of citizens connected to electronic devices. Whether on one's phone or laptop, the knowledge that what they enter into these devices may be spied upon changes one's behavior. According to research conducted in this post-Snowden atmosphere, thirty-four percent of Americans familiar with the revelations have taken steps to shield their information from the government (Pew Internet). The revelations that the government can track what you search have made citizens more compliant by not searching certain information. Some twenty-six percent of people who have heard a "lot" about surveillance use social media less often and change their social media privacy settings (Pew Internet). Some sixty-one percent of Americans, "say they have become less confident the surveillance efforts are serving the public interest" (Pew Internet). Furthermore, fifty-four percent of Americans believe it is unacceptable to monitor Americans under this dragnet approach (Pew Research Center). These revelations also contributed to feeling less confident in the security of common communication channels like social media that they suspect are heavily monitored by the government (Pew Research Center). Eighty-one percent feel "not very" or "not at all secure" when using social media sites to share personal information (Pew Research Center). This trend bodes ill for the future of dissent in America, when organizing and coordinating protests over digital devices are unprotected knowledge and may detract citizens from engaging in behavior that is not illegal, but frowned upon by government

agencies. Moreover, this trend of self-censorship is the ultimate victory of a panopticon that seeks to instill fear to ultimately citizens' behavior and make them compliant, obedient and conforming to state expectations (Greenwald, 175).

Conclusion

The uninhibited control of the Internet by American intelligence agencies directly contradicts the values of a democratic government. Despite the security justifications for such intrusive surveillance programs, an independent report found that the mass collection of phone metadata, codified by Section 215, had not stopped any terrorist attacks or plots (9/11 Commission Report: Privacy and Civil Liberties Oversight Board). The framework for massive surveillance touches every facet of a citizen's life in the twenty-first century, when life and work take place largely online. With the effects of a panopticon already instilling fear and compliance in the U.S. citizenry, efforts must be made to restructure, if not completely dissolve, the ineffective surveillance state. Although it may be impossible to "reset the Net," technology companies are changing their practices to meet the public's demands for stricter privacy in the post-Snowden era. As a result, companies like Apple are making encryption standard on their devices, much to the dismay of law enforcement and intelligence agencies (Nakashima and Gellman). Snowden's revelations uncover that the Internet has been coopted into a perfect tool of control for American intelligence agencies with dangerous implications for the vibrancy of a democracy in which every aspect of life can be and is digitized. Although political life is not as restricted as in China, the policies and techniques used by American intelligence agencies are remarkably similar to their China counterparts. Both presume that political activity threatens the prevailing order and issue blanket surveillance to protect their power. Both promote a political atmosphere of compliance with their direct and indirect means of surveillance that encourages

self-censoring behavior. Both enjoy high levels of stability that reduce the political efficacy of dissent via digital technologies.

Chapter 6: Conclusion

Despite the varied use of ICTs in these four case studies, a striking common unifier is present: ICTs are manipulated and designed as a tool of control by the state to protect its political power. The hidden form of technology that is conducive to control is the data produced by ICTs. This data tells a lot about a user; it tracks what a person communicates and thinks and where he, or she goes. Thus ICTs enable the CCP to practice censorship and surveillance techniques as grounds for detainment, or suspicionless surveillance to reinforce their power and legitimacy. The ingenuity of this approach is that ICTs perceive a wave of democratization that is not completely accurate, but rather illusionary. In China, dissent opinions are corrected and repressive tactics are employed once there is a concerted effort to disrupt the power of the Party. During the Arab Spring, the promise of ICTs as democratizing forces sputtered after continued military repression throughout political instability. Egypt's chaotic order continues to repress its people and several hundreds of protesters were killed in the latest uprisings in 2013. Thus, in China and Egypt the censorship and surveillance of ICTs is reinforced by physical repression. Hence the liberalizing effects of the Web are controlled in China as a façade of democracy. In Egypt, ICTs cannot solve the political problem of political fragmentation, and may in fact ignite further conflict. Additionally, the U.S. control of ICT data raises the question of whether, or not such mediums of communication are given the same democratic rights as non-digital speech.

Are ICTs a force of democratization?

There are considerable liberalizing effects from ICTs in each of the case studies; information is shared quickly and easily. Yet what these studies also prove is that ICTs do not generate political power from below, or from sources other than the state. In other words, the cyber-utopian mixture of ICTs and existent alternative political spheres has had little effective

political change. The widespread use of ICTs by citizens makes it an attractive medium through which political discourse can flow; yet in China and Egypt, collective movements disintegrate thanks to state technological repression, and in other cases, physical repression. The Arab Spring in Egypt successfully disposed a tyrant, but the ICTs and the remaining political groups could not solve the political problems of unifying Egypt under a rule that was not dictatorial and established. While in the U.S. the political atmosphere is democratic, so the focus of ICTs in this context should reinforce democratizing power. Yet political change via grassroots mobilizations is sparse and ineffective when demonstrated. While the mass surveillance state erected to capture and find terrorists detracts from liberty of citizens, these dragnet systems still pervade all electronic communications.

The sole objection to the weak power ICTs generate is the emergence of the hacktivist as an outlying actor between a citizen and state. Members of Anonymous possess highly sophisticated use of ICTs that parallels, and may even surpass, some states' use of these tools. However, the promise thought to be embedded in ICTs was that everyone could use them to bring about political change and democratize the world one wired authoritarian regime at a time. Instead, the common citizen uses ICTs for communication and coordination. Non-violent protest and dissent may be amplified, but muster little political change. Whereas, Anonymous' use of sophisticated ICT weapons, like DDoS attacks, allows it to initiate public outcry, and sometimes, political change, yet outside the levers of government.

The biggest lesson to take from this thesis is how the unveiling of a mass domestic surveillance system flips the original question of this thesis of whether ICTs are forces of democratization. Instead, ICTs are forces of control, which infringe on citizens' liberties to varying extents, depending on the political context. The case studies focusing on China and

Egypt demonstrate the effectiveness of ICT collection in preserving political power and staving off potential threats to that power, whether it manifests digitally or on the streets. Additionally, the repression associated with activists—both digital and on the streets—encourages apolitical behavior in both mediums. Whereas, ISIS uses ICTs like videos and spam tweeting as a Spinternet that builds the creation narrative of the fledgling state as to evoke fear regionally and globally and gain political power. It is to be expected that non-democratic actors seek preservation of power because they hold power mandate, but rule and keep order via some sort of force. However, even democratic nations —U.S., Canada, U.K., Australia, and New Zealand—engage in mass surveillance because it is the most pervasive form of control to protect power.

This assimilation between democratic and non-democratic regimes in terms of using ICTs as forces of control is concerning but is also steeped in the reality of data byproducts emitted by ICTs. The digitization of culture and politics fulfills the ICTs' potential as an unprecedented tool of control via the allure of technology. The wide-scale adoption of ICTs like smart phones inevitably produce sensitive, personal data, which are the center of state ICT control although they such information appears non-threatening. Simply put, we do not understand, or foresee, how the data we willingly relinquish can be used to control us. With the convenience of digital age, there is an encroachment on one's privacy and autonomy. Lessig accurately theorized that the commercialization of the Internet was the definitive act towards making the Internet more closed. Today, technologies are equipped with GPS tracking, sensors and Wi-Fi that produce sensitive data on one's whereabouts, heart rate, communications, etc. This knowledge, if privy to companies and intelligence agencies, greatly facilitates the construction of a mass surveillance system. The NSA revelations undoubtedly contribute to

making this argument not only relevant, but also chillingly real. In the wake of the Snowden revelations, U.S. technology companies are facing a challenge in foreign markets in which they are perceived as collusive with the government (Hakim). This development inverts Lessig's original thinking that commerce designs a Net that is conducive to control; rather governments promote ICTs as a form of control (Lessig, 37).

Now technology companies are implementing more protective measures of their clients' data. In their latest operating system update, Apple now encrypts all its iMessages (Apple). This idea is evident in chapter three when Robert Hannigan argues that technology companies abet terrorism by allowing such organizations, like ISIS, to enjoy the connectivity of the Web without being tracked. Hannigan seems to be saying two demands: take ISIS off Twitter and stop creating encryption to make data impenetrable. As stated in chapter three, ICTs like Twitter, are tools that have the potential to be exploited, which is a cost of ensuring an open society and Web. Secondly, Hannigan's argument for weaker encryption disregards the ethical concerns of mass surveillance. Instead Hannigan favors the extension of the dragnet in order stop terrorist attacks without considering the ineffectiveness of mass surveillance, especially when compared to traditional law enforcement and targeted surveillance methods. These are the types of problems that characterize the title of this thesis, as "Power Tangled in the Web;" how the growing concern over what happens with one's data is belittled by the state and commerce.

Why this Matters

What ultimately eviscerates social media networking sites and ICTs' potential generally is how what they post or tweet is conducive to collection and control. Perceiving ICTs as a collection vacuum effectively de-incentivizes users from communicating pertinent or political information over the web. This act of self-censorship and digital reclusion is becoming evident in

research. Pew Research Center found in August 2014 that social media does not provide an alternative, vibrant sphere for political talk when focusing on the Snowden revelations: "People reported being less willing to discuss the Snowden-NSA story in social media than they were in person—and social media did not provide an alternative outlet for those reluctant to discuss the issues in person" (Pew Research Center). No longer is the hidden control of ICTs ambiguous; the digitization of everything enables control and changes the way we perceive technology. If users of social networking sites are hesitant to engage in political discussion on Facebook, how can ICTs invoke political change? Thus, power is tangled in the Web; citizens are hesitant to contribute on ICTs that leave their data vulnerable, and states engaged in mass surveillance rely on the continued stream of data by compliant, uninformed or lazy users. The convenience of ICTs and their firm embedment in culture demands a solution to the unnecessary and anti-liberalizing effects of a mass surveillance system. In the political context of the U.S. mass surveillance state the use of ICTs is paradoxically antithetical to liberty.

Although political change may be more accessible within the levers of government in the U.S., the use of ICTs as a vehicle for political change is unfounded in all four studies. Instead, each study revealed how ICTs are a revolutionizing form of control, when a state can mitigate the inevitable liberalizing effects. China's masterful use of the Web brings about positive changes in terms of increased responsiveness to its citizens about local corruption and environment problems. Yet the control of ICTs ensures that any significant political challenges will be identified and suppressed before gaining traction. ISIS seeks to control how the world perceives it as a legitimate state. In a matter of time, ISIS will be able to employ sophisticated ICT censorship and surveillance to further incubate its power, like China, Egypt and the U.S.

Egypt and the U.S. both use ICTs to control political grassroots movements and respond in ways to suppress the power of ICTs, indirectly in the U.S. study and directly in the Egyptian case.

Like Lessig feared, ICTs have been left to themselves, or rather, left to the discretion of the state and became the most invasive tool of control yet. Apart from traditional surveillance, digital surveillance can know your most private details of what you are thinking, based off your data byproducts. With this power is confined to those in political power, ICTs effectively suppress liberty rather than promoting it. Until more safeguards are implemented to protect against the manipulation of ICTs, the perception of liberalizing ICT power, from the citizen perspective, will ultimately favor whoever controls all the data: states and technology companies. In this regard, political power in the Web is not tangled; it is clearly in the interest of the state. Whereas, citizen power via ICTs is tangled; if one uses these technologies they submit to a pervasive, inescapable system of control. If they opt out of ICTs, they cannot function in the day-to-day demands of life in the twenty-first century. This is evident in the failure of digital mass mobilizations, like the 2011 Egypt uprisings and the Occupy movement, to produce actual political change with the help of ICTs, but is ultimately restrained by physical and digital repression. Yet technology is the result of human processes. Thus, if users can initiate different policies to ensure that ICT tracking is not the de facto setting in non-democratic and democratic regimes alike, then perhaps "liberation technology" will prosper. Until then, ICTs act more like "suppression technology" to varying degrees, although each case study demonstrates how each example of state ICT control are all uniformly chilling to liberty.

Works Cited

Al-Hayat Media Center. "ISIS New Propaganda Video - John Cantlie Report From Mosul, Iraq." YouTube, 5 Jan. 2015.

Al-Jazeera Fault Lines Documentary, "History of an Occupation," 21 March, 2012.

Al-Jazeera English "Syrian Troops Beheaded in Raqqa," July 26, 2014.

Andelman, David A. "The Art of Dissent: A Chat with Ai Weiwei." *World Policy Journal* 29.3 (2012): 15-21.

Ansfield, Jonathan. "China Web Sites Seeking User Names." *The New York Times*. 5 Sept. 2009.

Ansfield, Jonathan. "Chinese Authorities Putting Pressure on Business to Help Censor the Web." *The New York Times*. 13 Nov. 2012.

Apple. "We've built privacy into the things you use everyday." *Apple* website. 2014.

Arango, Tim, and Eric Schmitt. "Escaped Inmates From Iraq Fuel Syrian Insurgency." The New York Times, 12 Feb. 2014.

Arango, Tim, Alicia Parlapiano, and Suadad Al-Salhy. "How ISIS Works." *The New York Times* 15 Sept. 2014.

Beam, Christopher. "Hong Kong's Own Reddit Is Doing the Protesters' Dirty Work—Sometimes Too Dirty." *New Republic*, 15 Oct. 2014.

Beech, Hannah. "Michelle Obama Defends Free Internet in China Speech." Time, 22 Mar. 2014.

Berger, J.M., and Jonathon Morgan. "Defining and Describing the Population of ISIS Supporters on Twitter." *The Brookings Institution, Center for Middle East Policy*. U.S. Relations with the Islamic World, No. 20. 05 Mar. 2015.

Bowker, Robert. "Egypt: Diplomacy and the Politics of Change," Middle East Journal; Autumn 2013, Vol. 67 Issue 4, p580

Castells, Manuel. *Networks of Outrage and Hope : Social Movements in the Internet Age*. Cambridge, UK; Malden, MA: Polity, 2012.

Coleman, E. Gabriella. *Coding Freedom :The Ethics and Aesthetics of Hacking*. Princeton: Princeton University Press, 2013.

Diamond, Larry Jay. Plattner,Marc and et al. *Liberation Technology : Social Media and the Struggle for Democracy*. Baltimore, Md.: Johns Hopkins University Press, 2012.

Doyle, Aaron. "Revisiting the Synopticon: Reconsidering Mathiesen's 'The Viewer Society' in the Age of Web 2.0." *Theoretical Criminology* 15.3 (2011): 283-99.

"Egypt: Egyptian Policeman Charged Over Shooting of Protester." *Asia News Monitor*: n/a. Mar 20, 2015 2015. *ProQuest Newsstand.*

"Egypt Internet Access." Internet Monitor. Harvard, Berkman Cyberlaw Center.

"Enemies of the Internet," Reporters Without Borders, 12 Mar. 2012.

Forsythe, Michael and Wong, Alan, "On TV, Hong Kong Openly Debates Democracy." *New York Times*, Wednesday, 22 Oct. 2014.

Friedman, Thomas. "The Five Myths." *Chinese American Forum* 16.3 (2001): 30-.

Gane, Nicholas. "The Governmentalities of Neoliberalism: Panopticism, Post-Panopticism and Beyond." *SORE The Sociological Review* 60.4 (2012): 611-34.

Gladstone, Rick. "Activist Links More Than 26,000 Twitter Accounts to ISIS." *The New York Times*, 31 Mar. 2015.

Gladstone, Rick, and Vindu Goel. "ISIS Is Adept on Twitter, Study Finds." *The New York Times*, 05 Mar. 2015.

Gladwell, Malcolm. "Small Change: Why the Revolution Will Not be Tweeted." *The New Yorker* Oct. 4, 2010.

Goldsmith, Stephen, Susan Crawford, and Michael Bloomberg. *The Responsive City :Engaging Communities through Data- Smart Governance*. San Francisco, California; 4: Jossey-Bass, 2014; 2014.

Gong, Li. "China's Unofficial Democracy." *Nature* 461.7265 (2009): 731-.

Goode, Luke. "Anonymous and the Political Ethos of Hacktivism." *Popular Communication* 13.1 (2015): 74-86.

Greenwald, Glenn. *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. New York, NY: Metropolitan Books/Henry Holt, 2014.

Haiqing Yu. "From Active Audience to Media Citizenship: The Case of Post-Mao China." *Social Semiotics* 16.2 : 303-26.

Hakim, Danny. "Google is Target of European Backlash on U.S. Tech Dominance." *The New York Times*. 8 Sept. 2014.

Hannigan, Robert. "The Web Is a Terrorist's Command-and-control Network of Choice." *Financial Times*. 3 Nov. 2014.

Howard, Philip N., Hussain, Muzammil M. *Democracy's Fourth Wave? : Digital Media and the Arab Spring*. Oxford; New York: Oxford University Press, 2013.

Howard, Philip N. *The Digital Origins of Dictatorship and Democracy: Information Technology and Political Islam*. Oxford; New York: Oxford University Press, 2010.

Howard, Philip N., and Muzammil M. Hussain. *State Power 2.0; Authoritarian Entrenchment and Political Engagement Worldwide*. Surrey, England; Burlington, Vermont; 4: Ashgate Publishing Company, 2013.

Hua, Cheng. "When an Open Internet is Closed." *New Statesman* 141.5128 (2012): 12-3. Web.

Isaacson, Walter. *The Innovators: How a Group of Hackers, Geniuses, and Geeks Created the Digital Revolution*. New York, NY: Simon & Schuster, 2014.

Izadi, Elahe. "American Teenager Charged with Trying to Fly Overseas to Join Islamic State." *Washington Post*, 6 Oct. 2014.

Jacobs, Andrew. "Chinese Web Censors Struggle With Hong Kong Protest." *The New York Times*, 30 Sept. 2014.

Jiao, Priscilla. "Beijing Clarifies Internet Policy, Defends Curbs; Controls on Net Required for 'State Security'." *South China Morning Post*, sec. NEWS: 04. June 9 2010.

Jumet, Kira D. "The Egyptian Uprisings from 2011 to 2013: Who Says they were about Democracy?" *Conference Papers -- American Political Science Association* (2014): 1-28.

Khan, Adnan R. "On the Road to Terror." *Maclean's* 127.37 (2014): 29-31.

King, Gary, Jennifer Pan, and Margaret E. Roberts. "How Censorship in China Allows Government Criticism but Silences Collective Expression." *American Political Science Review* 107.2 (2013): 326-43.

Lei, Ya-Wen. "The Political Consequences of the Rise of the Internet: Political Beliefs and Practices of Chinese Netizens." *Political Communication* 28.3 (2011): 291-322.

Leibold, James. "Blogging Alone: China, the Internet, and the Democratic Illusion?" *Journal of Asian Studies* 70.4 (2011): 1023-41.

Lessig, Lawrence. *Code version 2.0.* 2006.

Li, Shubo. "The Online Public Space and Popular Ethos in China." *Media, Culture & Society* 32.1 (2010): 63-83.

Liang, Bin, and Hong Lu. "Internet Development, Censorship, and Cyber Crimes in China." *Journal of Contemporary Criminal Justice* 26.1 (2010): 103-20.

Lyon, David. "An Electronic Panopticon? A Sociological Critique of Surveillance Theory." *Sociological Review* 41.4 (1993): 653-78.

MacKinnon, Rebecca. "China's "Networked Authoritarianism". *Journal of Democracy* 22.2 (2011): 32-46. Print.

MacKinnon, Rebecca. *Consent of the Networked: The Worldwide Struggle for Internet Freedom*. New York: Basic Books, 2012.

Miller, Vincent. *Understanding Digital Culture*. London; Thousand Oaks, CA: Sage, 2011.

Moore, Malcolm. "China Cuts Off Internet Access in Bid to Exert Control; as the Chinese Government Continues to Tighten its Control Over the Internet, the Country Became an Island for Roughly an Hour on Thursday, with all Access to Websites Beyond its Borders Cut Off." *Telegraph.Co.Uk,* April 12 2012.

Morozov, Evgeny. *The Net Delusion :The Dark Side of Internet Freedom*. 1st ed. New York, NY: Public Affairs, 2011.

Nordland, Rod. "Iraq's Sunni Militants Take to Social Media to Advance Their Cause and Intimidate." *The New York Times*, 28 June 2014.

Perlez, Jane. "In Beijing Talk, Michelle Obama Extols Free Speech." *New York Times* 163.56449 (2014): 4-.

Pieterse, Jan Nederveen. "Leaking Superpower: WikiLeaks and the Contradictions of Democracy." *Third World Quarterly* 33.10 : 1909-24.

Pollock, John. "Streetbook." MIT Technology Review, 23 Aug. 2011.

Postman, Neil. *Technopoly :The Surrender of Culture to Technology*. New York: Knopf, 1992.

Postman, Neil. "College Lecture Series - Neil Postman - "The Surrender of Culture to Technology"" *YouTube*, 11 Mar. 1997.

Rainie, Lee and Mary Madden. "Americans' Privacy Strategies Post-Snowden." *Pew Research Center*. 16 March 2015.

Rhoads, Christopher, and Geoffrey A. Fowler. "Turmoil in Egypt: Government Shuts Down Internet, Cellphone Services." *Wall Street Journal*: A.11. Jan 29, 2011. *ProQuest Central.*

Robertson, Andy., Dragonetti, John., Sinkler, Scott., Krauss, Dan., Else, Lincoln., Knappenberger, Brian.,Luminant Media (Firm),. *We are Legion the Story of the Hacktivists*. [Marina Del Rey, Calif.]: Luminant Media, 2012.

Ryan, Johnny. *A History of the Internet and the Digital Future*. London: Reaktion, 2010.

Salamey, Imad. "Post-Arab Spring: Changes and Challenges." *Third World Quarterly* 36.1 : 111-29.

Salvatore, Armando. "New Media, the 'Arab Spring,' and the Metamorphosis of the Public Sphere: Beyond Western Assumptions on Collective Agency and Democratic Politics." *Constellations: An International Journal of Critical & Democratic Theory* 20.2 (2013): 217-28.

Scuitto, Jim. "ISIS Has between 20,000 and 31,500 Fighters, CIA Says." CNN. Cable News Network, 12 Sept. 2014.

Schenier, Bruce. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. W.W. Norton & Company. 2015.

Seeberg, Peter. "Guest Editor's Introduction: An Arab World in Transition, Political Changes and Theoretical Discussions in a Post-'Arab Spring' Scenario." *Middle East Critique* 24.1 (2015): 1-7.

Severance, Charles. "Vint Cerf: A Brief History of Packets." *Computer* 45.12 : 10-2.

Shane, Scott, and Ben Hubbard. "ISIS Displaying a Deft Command of Varied Media." *The New York Times*, 30 Aug. 2014.

Shen, Fei, et al. "Online Network Size, Efficacy, and Opinion Expression: Assessing the Impacts of Internet use in China." *International Journal of Public Opinion Research* 21.4 (2009): 451-76.

Sifry, Micah L. *Wikileaks and the Age of Transparency*. O/R Books, New York. 2011

Simpson, Peter. "Chinese Internet Users Surges Past Half a Billion; the Number of Internet Users in China has Surged Past Half a Billion and Online Citizenship Continues to Grow Fast, According to Latest Figures." *Telegraph.Co.Uk*January 17 2012.

Smith, Aaron. April, 2015, "The Smartphone Difference." *Pew Research Center*.

Stoll, Clifford. *The Cuckoo's Egg :Tracking a Spy through the Maze of Computer Espionage*. New York, N.Y.: Pocket Books, 1990.

Strafella, Giorgio, and Daria Berg. "“Twitter Bodhisattva”: Ai Weiwei’s Media Politics." *Asian Studies Review* 39.1 : 138-57.

Tang, Lijun, and Helen Sampson. "The Interaction between Mass Media and the Internet in Non-Democratic States: The Case of China." *Media, Culture & Society* 34.5 (2012): 457-71.

Taylor, Astra. *The People's Platform: Taking Back Power and Culture in the Digital Age*. Fir ed. New York, New York: Metropolitan Books, Henry Holt and Company, 2014.

"The Internet in China - China.org.cn." Information Office of the State Council of the People's Republic of China. Beijing 8 June 2010.

"The US 9/11 Commission on Border Control." Population and Development Review 30.3 (2004): 569-74.

The Rise of ISIS. PBS Frontline, 2014. Documentary.

USA PATRIOT Act. Title II: Section 215. 2001

Tze-wei, Ng, and Kristine Kwok. "Beijing Snaps Back at Clinton Internet Criticism." *South China Morning Post*, sec. NEWS: 04. January 23 2010.

Ward, Clarissa. "Campaigning for ISIS in the West." *60 Minutes*. CBS Interactive, 2 Nov. 2014.

Ward, Clarissa. "Former ISIS Member Explains Why He Left Terror Group." CBSNews. CBS Interactive, 9 Feb. 2015.

Wei Wei, Ai. *Ai Wei Wei's Blog*. Tran. Lee Ambrozy. Ed. Lee Ambrozy. Cambridge: Massachusetts Institute of Technology, 2011.

Wolfson, Todd. *Digital Rebellion :The Birth of the Cyber Left*. Chicago: University of Illinois Press, 2014.

Wood, Graeme. "The Secrets of ISIS." *New Republic* 245.15 (2014): 14-7.

World Trade Press. *Egypt Media, Internet and Telecommunications Complete Profile*. Petaluma, CA, USA: World Trade Press, 2010.

Wu, Tim. *The Master Switch: The Rise and Fall of Information Empires*. New York: Alfred A. Knopf, 2010.

Yang, Guobin. The Power of the Internet in China: Citizen Activism Online. New York: Columbia UP, 2009. Print.

Zhai, Keith. "Wall Comes Down Briefly for Facebook Users." *South China Morning Post*, sec. NEWS: 06. April 25 2012.

Zittrain, Jonathan, and Lawrence Lessig. *The Future of the Internet and how to Stop it*. New Haven Conn.: Yale University Press, 2008.

Zurayk, Rami and Anne Gough. “Bread and Olive Oil: The Agrarian Roots to the Arab Uprisings.” *The New Middle East: Protests and Revolution in the Arab World*. Ed. Fawaz A. Gerges.

Acknowledgments

First and foremost, I would like to thank my thesis advisor, Professor Chubb, for her guidance throughout this thesis project and my time at Holy Cross. If it had not been for her *Comparative Politics* course in the fall of my freshman year in 2011, I would not have pursued the Political Science major or this thesis. Professor Chubb's untiring amount of patience and grammatically sound edits were instrumental in making my ideas into a hundred pages of text. Additionally, I would like to thank Professor Klinghard for his assistance in navigating me through a vast amount of technology literature that was extraordinarily helpful for my first chapter. Professor Klinghard's *Politics and Technology* seminar was a formidable part of my undergraduate career experience, and the ideas I encountered in that class are woven into these pages. Thank you, Professor Rodrigues for reading my thesis and providing valuable insight and commentary on the erosion of social capital in this digital age. Thank you to Professor Brand and the entire Political Science department for supporting my thesis prospectus last spring and through its fulfillment a year later. Thank you to the staff at Dinand Library who have supplied me with every book and article I have requested and for making this thesis accessible to everyone in the world, with an internet connection, via Crossworks. Thank you to all my professors throughout my four years at Holy Cross that have shaped me as a person and a student. Lastly, thank you to my family and friends who have encouraged throughout this entire process and inspired me to analyze how technology affects our lives and politics.